P517531.PDF [Page: 3 of 85]

DEFENCE R&D DÉFENSE

A Security Analysis of Windows 2000 Group Policies

J. Savoie

Defence R&D Canada

TECHNICAL MEMORANDUM
DREO TM 2001-084
November 2001

National Defence / Défense nationale

Canada

PS17531.PDF [Page: 4 of 85]

REPRODUCTION QUALITY NOTICE

This document is the best quality available. The copy furnished to DRDCIM contained pages that may have the following quality problems:

: Pages smaller or Larger than normal

: Pages with background colour or light coloured printing

: Pages with small type or poor printing; and or

: Pages with continuous tone material or colour photographs

Due to various output media available these conditions may or may not cause poor legibility in the hardcopy output you receive.

☒ If this block is checked, the copy furnished to DRDCIM contained pages with colour printing, that when reproduced in Black and White, may change detail of the original copy.

P517531.PDF [Page: 5 of 85]

105-03266/

A Security Analysis of Windows 2000 Group Policies

J. Savoie
Defence Research Establishment Ottawa
Information Operations Section

Defence Research Establishment Ottawa

Technical Memorandum

DREO TM 2001-084

NOVEMBER 2001

PS17531.PDF [Page: 6 of 85]

© Her Majesty the Queen as represented by the Minister of National Defence, 2001

© Sa majesté la reine, représentée par le ministre de la Défense nationale, 2001

Abstract

In this technical memorandum, we analyse the security-relevant Windows 2000 policies that can be set up on Windows 2000 domains and show how these policies are applied and implemented. These policies are a large set of authentication policies, password policies, application policies, installation policies, and others.

This analysis is a first step needed before setting up the Windows 2000 policies for one or more secure domain demonstrators for the Canadian Forces and other organisations where normal users would be low power users to mitigate risk on domain assets.

Résumé

Dans ce memorandum technique nous analysons les politiques de sécurité qui s'appliquent aux ordinateurs membres d'un domaine Windows 2000 et montrons comment ces politiques sont appliquées et implantées. Ces politiques de sécurité sont composées de plusieurs types de politiques dont des poliques d'authentifications, de mots de passe, d'applications et d'installations.

Cette analyse est une première étape avant d'établir une politique de sécurité pour un ou des prototypes de domaines Windows 2000 pour les Forces Canadiennes et autres organisations où les usagers seront des usagers ayant peu de privilèges. Tout ceci dans le but de diminuer les risques sur les élements protégés par ces domaines.

P517531.PDF [Page: 6 of 85]

This page intentionally left blank

Executive summary

The Canadian Forces, as other small or large organisations, aim to protect their network data against destruction and disclosure, and keep their operational capacity against network attacks caused by viruses, Trojan Horses, denial of service attacks, and network penetrations.

Network domains such as Netware , Windows NT 4.0, and Windows 2000 domains are tools used by organisations to protect and share their data. In this technical memorandum, we analyse the Microsoft-provided security policies that a domain administrator can set up to protect a Windows 2000 domain and show how these policies are applied and implemented. These policies consist of authentication policies, password policies, application policies, installation policies, and others.

Not only are policies for Windows 2000 domains interesting because they extend policies for Window NT 4.0 domains, they also allow system administrators to set up domains in which simple users can work with few privileges and rights. This fact is very important because Windows NT 4.0 users are usually much too powerful. For example, when a program runs on behalf of a user with system administrator rights and privileges, it can modify system files and settings and install malicious services. Thus, by limiting normal users privileges and rights in a domain, it becomes possible to protect computer systems against malicious programs run on behalf of simple users. Moreover, it becomes possible using Windows 2000 policies to install and configure applications centrally. Hence, users can be limited to work in an environment where they cannot install applications and/or modify applications security parameters.

Even though Windows 2000 policies provide solutions for protecting users from themselves, they don't prevent this risk completely because users can run malicious programs that don't need to be installed. In summary, Windows 2000 policies are useful to protect system resources and application settings but malicious programs can harm users' resources.

This memorandum is intended to provide initial information and considerations prior to define sets of Windows 2000 policies for one or more secure domain demonstrators. We later intent to build one or more domain demonstrators to provide examples of secure Windows 2000 domains that could be used by the Canadian Forces and other Canadian government organisations.

Savoie, J. 2001. A Security Analysis of Windows 2000 Group Policies.
DREO TM 2001-084. Defence Research Establishment Ottawa.

PS17531.PDF [Page: 10 of 85]

Sommaire

Les Forces Canadiennes et autres organisations veulent protéger les informations contenues dans leurs réseaux informatiques tout en gardant ceux-ci fonctionnels lors d'attaques causées par des virus, des chevaux de Troie, des dénis de services, ou des penétrations de réseaux.

Les domaines pour les réseaux informatiques comme les domaines Netware, Windows NT 4.0, et Windows 2000 sont des outils utilisés par les organisations pour protéger et partager leurs données. Dans ce memorandum technique, nous analysons les politiques de sécurité qui peuvent être appliquées à des domaines Windows 2000 et montrons comment elles sont appliquées et implantées. Ces politiques contiennent un large éventail de politiques dont des politiques sur l'authentification, les mots de passe, les applications, et l'installation de logiciels.

Les politiques de sécurité pour les domaines Windows 2000 sont intéressantes non seulement puisqu'elles étendent les poliques pour les domaines Windows NT 4.0 mais aussi car elles permettent la construction de domaines où les usagers peuvent fonctionner tout en ayant peu de privilèges et droits. Ce fait est très important car les usagers de domaines Windows NT 4.0 sont trop souvent trop puissants ce qui introduit des vulnérabilitées pour les réseaux informatiques. Par exemple, lorsqu'un programme fonctionne sur un ordinateur au nom d'un usager qui a les droits et privilèges d'un administrateur de cette machine, ce programme peut modifier des fichiers systèmes et la configuration de l'ordinateur et peut installer des services malicieux. Ainsi, en limitant les privilèges et droits des usagers, il devient possible de protéger les fichiers systèmes et la configuration des ordinateurs contre les programmes malicieux fonctionnant au nom de simples usagers.

Le but de ce travail est une première étape avant d'établir une politique de sécurité pour des prototypes de domaines Windows 2000 qui pourront servir d'exemples pour de futurs domaines Windows 2000 des Forces Canadiennes ou autres organismes gouvernementaux.

Savoie, J. 2001. A Security Analysis of Windows 2000 Group Policies. DREO TM 2001-084. Centre de recherches pour la défense Ottawa

P517531.PDF [Page: 11 of 85]

Table of contents

Abstract i

Executive summary iii

Sommaire iv

Table of contents v

List of figures viii

1. Introduction 1

2. Windows NT 4.0 policies 4
   - 2.1 Loading of NT 4.0 policies 4
   - 2.2 Using the poledit.exe utility 5
   - 2.3 Adm files 6
   - 2.4 Inspecting security policy settings 6
   - 2.5 Limitations of Windows NT 4.0 policies 7

3. Group Policy Objects in Windows 2000 8
   - 3.1 Non-local GPOs 8
   - 3.2 GPO volatile registry keys 9

4. Client-side extensions and GPO processing 11
   - 4.1 Configuration data for client-side extensions 11
   - 4.2 GPO information cached by client-side extensions 13
   - 4.3 Extensions processing of GPOs 14

5. Microsoft Management Console (MMC) 16

6. Policies in Group Policy snap-in 18
   - 6.1 Windows Settings nodes 18
     - 6.1.1 Windows Settings in Computer Configuration node 19
       - 6.1.1.1 Policies in Account Policies node 20
       - 6.1.1.2 Policies in Local Policies node 20

P517531.PDF [Page: 12 of 85]

6.1.1.3 Policies in Event Log node 22
6.1.1.4 Policies in Restricted Groups node 22
6.1.1.5 Policies in System Services node 22
6.1.1.6 Policies in Registry node 22
6.1.1.7 Policies in File System node 22
6.1.1.8 Policies in Public Key Policies node 22
6.1.1.9 Policies in IP Security Policies node 23
6.1.2 Windows Settings in User Configuration node 23
6.2 Administrative Templates nodes 23

7. Computer Administrative Templates policies 25
7.1 Policies in Windows Components node 25
7.1.1 Policies in Task Scheduler node 26
7.1.2 Policies in Windows Installer node 27
7.2 Policies in System node 29
7.2.1 Policies in Logon node 30
7.2.2 Policies in Group Policy node 31
7.3 Policies in Network node 35

8. User Administrative Templates policies 37
8.1 Policies in Windows Components node 37
8.1.1 Policies in Microsoft Management Console node 38
8.1.1.1 Policies in Permitted/Restricted Snap-ins node 39
8.1.1.2 Policies in Extension Snap-ins node 39
8.1.1.3 Policies in Group Policy node 40
8.1.2 Policies in Windows Installer node 41
8.2 Policies in Start Menu & Taskbar node 42
8.3 Policies in Desktop node 43
8.4 Policies in Control Panel node 44
8.5 Policies in Network node 45
8.6 Policies in System node 47
8.6.1 Policies in Logon node 48
8.6.2 Policies in Group Policy node 49

P517531.PDF [Page: 13 of 85]

9. Internet Explorer 5.x security settings 50
9.1 User settings in Windows Settings node 50
9.1.1 Browser connections 51
9.1.2 Policies in Connection node 53
9.1.3 Policies in Security node 53
9.2 User settings in Administrative Templates node 54
9.2.1 Policies in Internet Control Panel node 55
9.2.2 Policies in Internet Explorer node 56
9.2.3 Policies in Offline Pages node 57
9.2.4 Policies in Browser menus node 57
9.2.5 Policies in Toolbars node 58
9.2.6 Policies in Persitance Behaviours node 59
9.2.7 Policies in Administrator Approved Controls node 60
9.3 Computer settings in Windows Settings node 60

10. Adm files 63
10.1 Editing and using adm files 63
10.2 Saving adm files 63

11. Conclusion 64

References 65

List of acronyms 66

P517531.PDF [Page: 14 of 85]

List of figures

Figure 1: The poledit.exe utility 5

Figure 2: Computer policy entrees 6

Figure 3: Non-local GPO's folder on DCs 9

Figure 4: Sample user GPO's volatile registry information 10

Figure 5: Extensions configuration data 11

Figure 7: GPO's information cached by a client-side extension 14

Figure 8: A Group Policy MMC console 17

Figure 9: Windows Settings nodes 19

Figure 10: Policies in Accounts Policies node 20

Figure 11: User Rights Assigment 21

Figure 12: Security Options 21

Figure 13: Computer Administratives Templates node 25

Figure 15: Nodes and policies in System node 30

Figure 16: Logon policies in System node 31

Figure 17: Group Policies policies in System node 32

Figure 18: Refresh sub-policies for Group Policy policies 32

Figure 19: The User Administrative Templates node 37

Figure 20: Policies in the MMC node 38

Figure 21: Policies in the Permitted/Restricted Snap-ins node 39

Figure 22: Policies in the Extension Snap-ins node 40

Figure 23: Policies in the Group Policy node 41

Figure 24: Policies in the Windows Installer node 41

Figure 25: Policies in the Sart Menu & Taskbar node 42

P517531.PDF [Page: 15 of 85]

Figure 26: Start button customisation dialog box 43
Figure 27: Policies in the Desktop node 44
Figure 28: Policies in the Control Panel node 45
Figure 29: Policies in the Network and Dial-up Connections node 45
Figure 30: The Network and Dial-up Connections window 46
Figure 31: Local Area Connection Properties dialog box 46
Figure 32: Advanced button 47
Figure 33: Nodes and policies in System node 47
Figure 34: Policies in the Logon node 48
Figure 35: Policies in the Group Policy node 49
Figure 36: User and computer settings for IE 50
Figure 37: Internet Explorer's LAN Settings page 52
Figure 38: Proxy Settings from the Advanced button 52
Figure 39: Administrative Templates\Internet Explorer node 54
Figure 40: Internet Options dialog box 55
Figure 41: Internet Control Panel policies 56
Figure 42: Offline Pages policies 57
Figure 43: Policies in Browser menus node 58
Figure 44: Toolbars policies 59
Figure 45: Toolbar Buttons selection 59
Figure 46: Administrator Approved Controls policies 60
Figure 47: Policies in Computer Internet Explorer node 61
Figure 48: Internet Options' Security tab 62

PS17531.PDF [Page: 16 of 85]

List of tables

Table 1. Extensions configuration data 12

Table 2. Names and actions of client-side extensions..... 34

P517531.PDF [Page: 17 of 85]

1. Introduction

Computer network security for organisations such as the Canadian Forces is becoming a primary concern. Organisations want to protect their data against destruction and disclosure, and keep their operational capacity against network attacks caused by viruses, Trojan Horses, denial of services attacks, and network penetrations.

System administrators in these organisations are facing the following problem: How does one provide users with a secure distributed environment that is usable, manageable, and affordable?

In order to solve this problem, system administrators can use the notion of domain for a group of computers and/or users. A domain is a security perimeter for a set of computers and users. This security perimeter is defined by the security policy that applies to all computers and users within the perimeter. The policy can be applied differently from one computer/user to another within the domain. An organisation may have one or more domains or share a domain with other organisations. The domain security policy may contain policies on authentication mechanisms, password length, configuration of communication protocols, allowed programs, etc.

There are different domain types. For instance, there are Netware domains, Windows NT 4.0 domains, and Windows 2000 domains. The notion of domain was first defined to provide authentication mechanisms. When a server authenticates a client, it can either use a local database or ask a trusted computer – called herein a domain controller – to authenticate the client. If no domain controllers are used, system administrators have to manage and/or replicate each local database, which become very complex. Therefore, domain controllers were first set up to provide centrally managed authentication mechanisms.

It is possible to associate more than just authentication mechanism policies to a domain. For example, for computers in a Windows NT 4.0 domain it is possible to set up system policies that are downloaded from domain controllers. These policies modify/write registry values of the computers. These values are thereafter used to configure users' programs and computer services. Policies for Windows 2000 domains extend policies for Windows NT 4.0 domains. Furthermore, a Windows-2000 extension mechanism is provided to Independent Software Vendors (ISVs) that allows them to create policies that apply to their software.

In this technical memorandum, we analyse the security-relevant Windows 2000 policies provided by Microsoft and show how these policies are applied and implemented. We assume that these policies are used to secure Windows 2000 domains containing only computers that use Windows 2000 policies. Windows-2000 or Windows-XP-Professional based computers are such computers. This analysis is intended to be a first step before setting up the Windows 2000 policies for one or more secure domain demonstrators. In a further work, we intent to build the domain

P517531.PDF [Page: 18 of 85]

demonstrators to provide examples of secure Windows 2000 domains that could be used by the Canadian Forces and other Canadian government organisations.

Windows 2000 policies are very interesting because they allow system administrators to set policies on a domain in which simple users can work with few privileges and rights. For Windows NT 4.0 domains, users usually need more privileges and rights because both Windows NT 4.0 programs often need more privileges to be run and users have to install software. It has been shown in [1] that current Windows NT 4.0 users are usually too much powerful because they are running their computers often as administrators or power users. Hence, when such a user clicks on a program icon, the started program runs with the user's privileges and rights.

For example, let us consider a user that is an administrator of a PC running Windows NT 4.0 or Windows 2000 operating system. After the user is logged on interactively to the PC, the system starts the program "Explorer" that is the user's interface to the system. The Explorer program runs with the user's security token that has administrator privileges and rights. When this user clicks on a program such as Word, Internet Explorer, or any other program the new program inherits by default the user's security token. If this program runs some malicious code, it can modify registry settings, delete/modify system files, installs Trojan Horses, etc.

Therefore, to provide users a secure workstation environment, system administrators have to make sure that:

- Users use only machines running secure Operating Systems (OSs). If there is no means to protect system files and/or system information, the system cannot protect itself from modification from low power users. Windows 95 or 98 doesn't provide file system security, so they cannot be considered secure OSs.

- Simple users should be low power users. Hence, if well configured, the system can protect itself from low power user modifications.

- Only trusted programs should be run. Even though the system is protected against low power users' actions, users need to be protected against themselves. If a user clicks on a malicious program for example, the program can delete user files or modify user configuration data. Therefore, users should run only trusted programs.

- Programs should be well configured. For example, Internet Explorer is a complex program that is linked to a Java Virtual Machine (JVM) that loads code remotely. This code can be malicious. Therefore, before executing this code, Internet Explorer must make sure that the code is trusted. To do that, it can ask, for example, either a trusted digital signature or a trusted location.

- Program configuration data that is security relevant should not be modifiable by low power users. Even though programs are well configured initially, if users can modify them later, the new configuration can be dangerous. It is often a difficult

PS117531.PDF [Page: 19 of 85]

task to determine the part of program configuration data that must not be modifiable by users.

- System administers should provide users the set of programs they need. Furthermore, they should provide these programs in a manageable way. In order to do that, it would be good to install users' programs remotely.

- System administrators should securely configure servers. Web servers, FTP servers, mail servers, and other servers need to be properly configured.

Windows 2000 policies can be of great help to system administrators for achieving that goal. In Windows 2000 domains where all computers and users are subject to a set of Windows 2000 policies, it becomes possible to design domains in which (1) users are low power and (2) application settings, service settings, and application installations are centrally managed and are outside of user control.

In this report we analyse mainly Windows 2000 policies that are security relevant. However, NetMeeting and IPSec policies are outside the scope of this work. Readers must be aware that we don't provide basic information on Windows NT 4.0 and Windows 2000 (see [2,3]). We assume also that readers know what registry keys are and how to locate them using the REGEDIT.EXE utility. The report findings were mainly based on [4] and experimentation on a small Windows 2000 domain. Moreover, [2, 3, 5] and numerous online publications provide other valuable information on Windows 2000 Group Policy.

The end of this section describes the report content. In Section 2, we give an overview on Windows NT 4.0 policies and show their limitations. In Section 3, we introduce the Group Policy Objects (GPOs) that implements the Windows 2000 policies. These objects are applied to sites, domains, and organisation units (OU). There are two types of GPOs: the local GPO that is located on the local computer and the non-local GPOs that are located on a domain controller. Some non-local GPOs are downloaded on a computer from a domain controller when a computer boots up, a user logs on, or during certain refresh time. In Section 4, we analyse the client-side extensions that are the components that process GPOs. We show how they are configured and how GPOs are processed. In Section 5, we give an overview on the MMC console that is the Windows 2000 universal system administrators' interface. Components added to an MMC are called snap-ins. In Section 6, we start the study of the current Microsoft Windows 2000 policies. The policies can be seen from an MMC console in which the Group Policy snap-in is added. In Section 7, 8, 9 we analyse the remaining Windows 2000 policies. Furthermore, we located in Section 9 all policies related to Internet Explorer to provide a better understanding of what can be done through policies for an important and complex application. In Section 10, we provide information on adm files that are used for a large set (450) of Windows policies. Adm files are also used by Windows NT 4.0 policies but are slightly different.

PS17531.PDF [Page: 20 of 85]

2. Windows NT 4.0 policies

In this section we first show how and when Windows NT policies are loaded on computers member of Windows NT 4.0 domains. Then, we introduce the poledit.exe utility that allows one to create adm files and policy files. Finally, we discuss some limitations of the Windows NT 4.0 policies.

2.1 Loading of NT 4.0 policies

Windows NT 4.0 policies are values loaded in the registry that are used by the operating system and applications while they initialise. Computers that are members of a Windows NT 4.0 domain are subject to a local policy and a System policy. When a Windows NT 4.0- based computer starts up, it loads some local files called hives that make the HKEY_LOCAL_MACHINE (HKLM) registry key. At this point, no files are downloaded from Domain Controllers (DCs) and the policy that applies to the computer is the local policy defined by some registry keys in HKLM . However, when a user logs on locally to the computer, new policies called System policies can be downloaded from domain controllers to modify/add registry settings. To do that, the system locates the UpdateMode value in the following registry key:

HKLM\SYSTEM\CurrentControlSet\Control\Update.

If the UpdateMode value is 0 (disabled mode), no System policies are downloaded and applied. If the value is either1 (automatic mode) or 2 (manual mode), the system tries to retrieve an Ntconfig.pol file. In automatic mode, the system searches NTconfig.pol in the Netlogon share on a domain controller while in manual mode it searches in one defined by the NetworkPath value located in the same registry key. The NetworkPath value is either a local path or a network share. No System policies are applied in the following four cases:

- The mode is automatic and the computer is not a member of a domain.
- The mode is manual and no NetworkPath value is defined.
- The NTconfig.pol is not present in the searched folder.
- The user has no read access to the NTconf.pol file.

Otherwise, the system applies the NTconfig.pol policies before logging on the user, which implies that the user cannot log on if the system cannot load the file.

Note: Consequently, if a group or a user is denied access to the NTconfig.pol file, the policy is not applied to that group.

P517531.PDF [Page: 21 of 85]

Note: It is possible to modify the UpdateMode value from a policy if the initial mode is automatic or manual. If the initial policy in a domain states a manual mode with no NetworkPath defined, the state of computers in the domain cannot anymore be modified from a new policy. In order to modify this behaviour, system administrators would have to modify the registry for each computer in the domain, which is a time consuming task. Therefore, before applying the first policy check that the initial policy doesn't state the manual mode with no NetworkPath defined.

2.2 Using the poledit.exe utility

Policy files such as NTconfig.pol are built through the poledit.exe utility. A policy is composed of different parts that apply to users, computers, and groups. Groups are only user groups. Figure 1 shows a sample policy that contains two specific users, a default user, two specific computers, a default computer, and three groups.

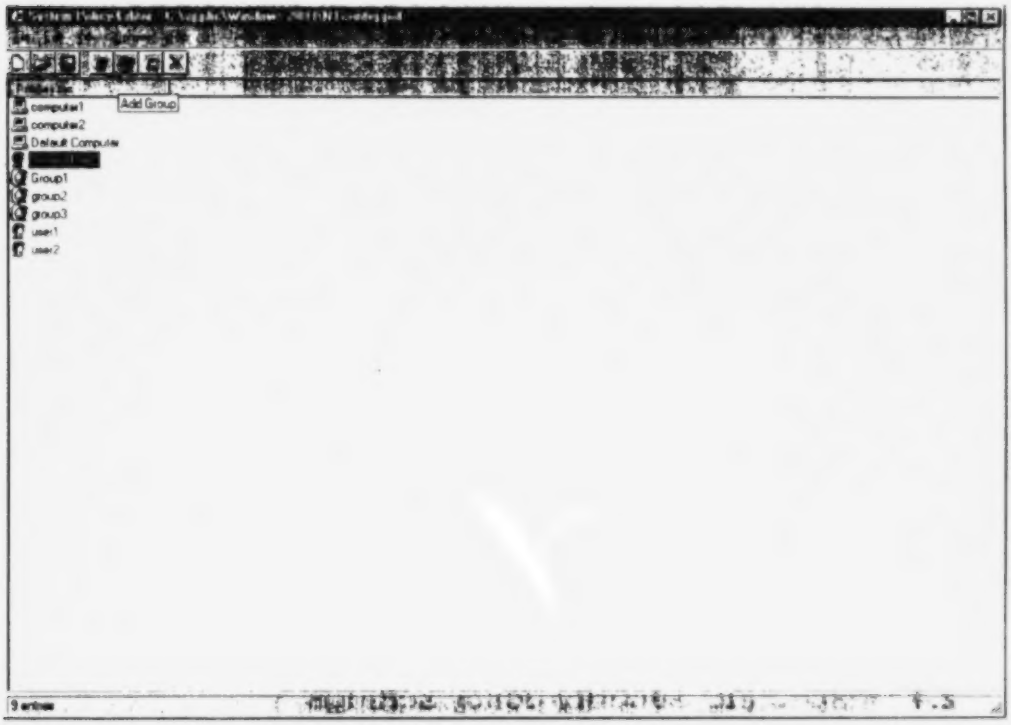

Figure 1: The poledit.exe utility

When a domain user logs on to a computer and a computer retrieves the NTconfig.pol file, the policy that applies to the user and computer is the one that is the most specific to the user and computer. More specifically, if the user has his policy defined, this is the user policy. If no user policy is defined and the user is member of at least one group policy, the user policy that applies is the one that has the highest group priority of those ones. If there are no groups that the user belongs to, the default

P517531.PDF [Page: 22 of 85]

user policy is the user policy. Similarly, if the computer has its own policy, this is the computer policy; otherwise, the default computer policy is applied.

2.3 Adm files

Adm files are text files used to create computer and user policies. These files are used by the poledit.exe utility to make pol files. Each policy stated in an adm file that is applied triggers a write in a registry key in either HKLM or HKEY_CURRENT_USER (HKCU). Computer policies write to HKLM while user policies write to HKCU. Figure 2 shows the computer policies for the previous sample policy. These policies are built from two adm files: common.adm and Winnt.adm.

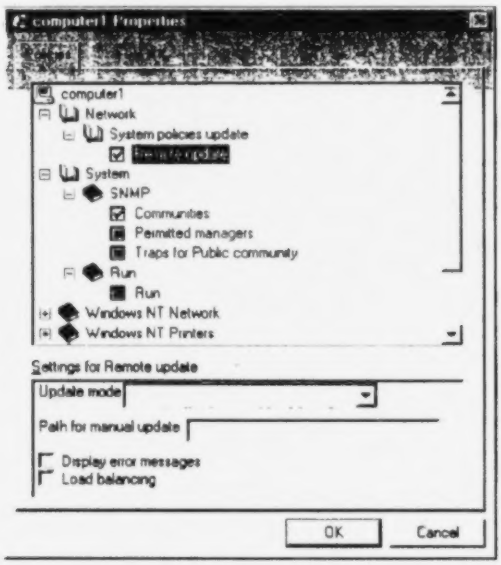

Figure 2: Computer policy entrees

2.4 Inspecting security policy settings

The poledit.exe utility allows us to display the registry settings for a given policy built on a set of adm files. In order to see the security setting of a given policy,

- Select Open Registry in the File menu
- Select Policy Templates in the Options menu and load the adm files defining the system policy that are not already loaded

P517531.PDF [Page: 23 of 85]

- Select Local Computer (Local User) to see the computer (user) security settings for the computer.

2.5 Limitations of Windows NT 4.0 policies

There are number of limitations to Windows NT-4.0 security policies. Firstly, when a system policy is applied to a computer, these settings remain in effect even after the local user is logged out. Consequently, the computer policy becomes the computer policy of the last locally logged on user. This can be a problem for multi-user computers because the computer policy can be unstable. Secondly, Windows NT 4.0 policies apply only to security settings controlled by the registry. It is not possible, for instance, to modify the security descriptor of NTFS files. Finally, it is not possible to apply a computer policy to computer groups.

3. Group Policy Objects in Windows 2000

A Group Policy object contains security permissions for Windows 2000-based computers. These permissions when applied provide the security settings for computers within a Windows-2000 domain. These settings depend on both the computer and the computer's logged on user – if there is one logged on. There are two types of Group Policy Objects (GPOs): local and non-local. These two GPO types are similar but their locations are different.

Each Windows 2000-based computer has a unique Local GPO that is located in *%systemroot%\system32\Group Policy* folder and some non-local ones that are located on domain controllers. GPOs extend local and system policies used for Windows NT 4.0-based computers. As Windows NT 4.0-based computers load or not system policy, Windows 2000-based computers load or not non-local GPOs from domain controllers depending on the UpdateMode key value in the HKLM\SYSTEM\CurrentControlSet\Control\Update registry key. Same comments about the UpdateMode values presented in Section 2 apply also.

A non-local GPO is associated to a site, a domain, or an Organisation Unit (OU) – a site is a set of IP addresses and an OU is a part of a domain in which administration duties can be delegated. The computer GPOs that apply to a computer are the computer local GPO and the computer GPOs of the computer's site, domain, and OU. Similarly, the user GPOs that apply to a computer when a user is logged on to the computer are the user local GPO and the user GPOs of the user's domain and OU.

In general, GPOs are applied to a computer in the following order: the local GPO, site GPOs, domain GPOs, and OU GPOs. Hence, computer/user policies that are effective are those that are the closest to the computer/user. That is, GPOs on OU override those on domains that override those on sites that override the local GPO. This default behaviour can be modified and has few exceptions. If a GPO is assigned to a site or a domain and has the no override flag, no lower level GPO can override this policy. Moreover, some policies apply only at the domain level. In that case, lower level polices are discarded.

3.1 Non-local GPOs

Each non-local GPO has a unique GUID (Globally Unique IDentifier) name. Each of them is stored in a folder that is replicated in all domain controllers in the domain. The folder name is the GPO's GUID name that is in the SYSVOL network share. Figure 3 shows a sample non-local GPO folder. It contains a GPT.INI file and the following three folders: Adm, Machine, and Users. The GPO version number is contained in the GPT.INI file, the Adm folder contains the adm files used by the Administrative Templates node in the Group Policy snap-in, and the machine and user folders contain respectively the computer and user policies.

P517531.PDF [Page: 25 of 85]

Note: The version information is the decimal representation of an eight-digit hexadecimal number. The four least significant digits represent the Computer Settings version number, and the four most significant ones represent the Users Settings version number. For example, if you see Version=65539, which is 0X00010003 in hexadecimal the Computer Settings and Users Settings version numbers are respectively 3 and 1.

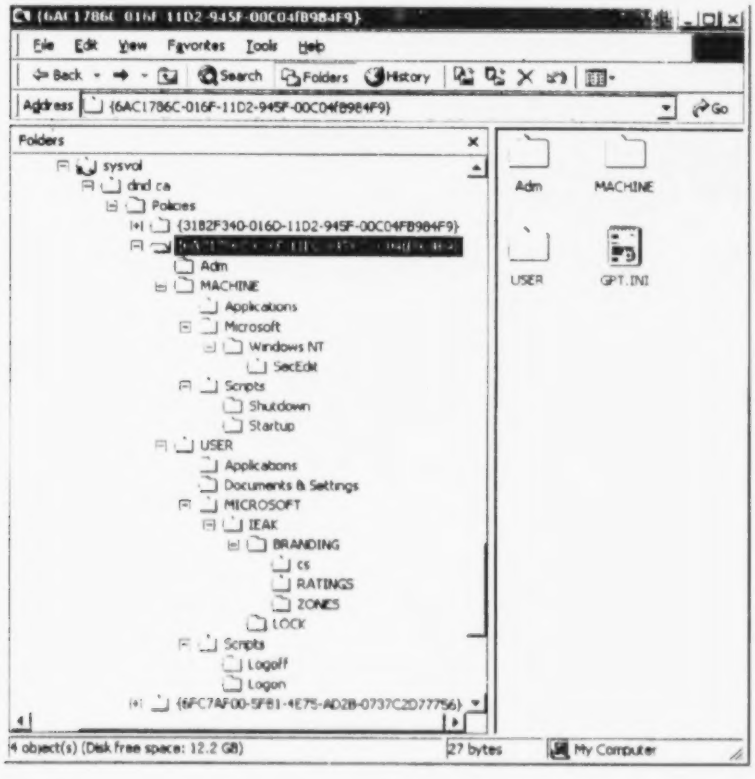

Figure 3: Non-local GPO's folder on DCs

3.2 GPO volatile registry keys

Some policies in GPO are policies that set values in the registry. These policies are called here GPO registry policies. Some of these policies store values in the four following registry keys in the local computer:

HKLM\Software\Policies

HKCU\Software\Policies

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies

P517531.PDF [Page: 26 of 85]

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies.

Since these keys are not stored in any hives on the local computer and so they are lost when the computer shuts down, they are called in this document GPO volatile registry keys.

For each non-local user or computer GPO, the GPO's information that is stored in volatile registry keys is also stored in \HKCU on domain controllers. Figure 4 shows a sample of this.

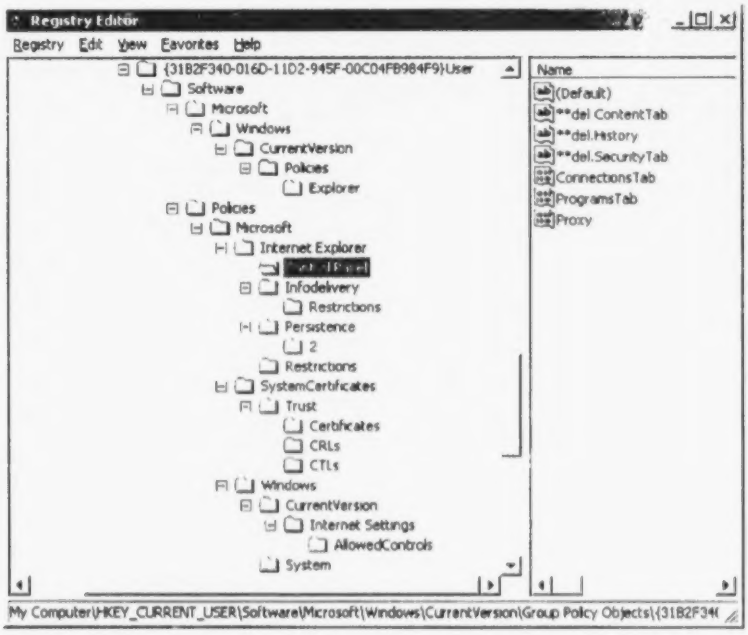

Figure 4: Sample user GPO's volatile registry information

P517531.PDF [Page: 27 of 85]

4. Client-side extensions and GPO processing

Client-side extensions are DLLs or system programs that process GPOs that apply to a computer when the system starts, a user logs on to the computer or the policy is refreshed. All of these computer GPOs and/or user GPOs are processed from the first to the last by each client-side extension. In this section we will show how client-side extensions get their configuration data, cache user and computer GPO information, and process GPOs.

4.1 Configuration data for client-side extensions

Each client-side extension is configured through a unique non-volatile registry key and a unique GPO volatile registry key. The non-volatile registry key is

HKLM\software\Microsof\Windows NT\CurrentVersion\Winlogon\GPExtensions\<*Client-side extension's GUID*>

Figure 5 shows in the left panel the non-volatile registry keys associated to client-side extensions for a Windows 2000-based computer. In the right panel, we can see the non-volatile configuration data for a sample client-side extension.

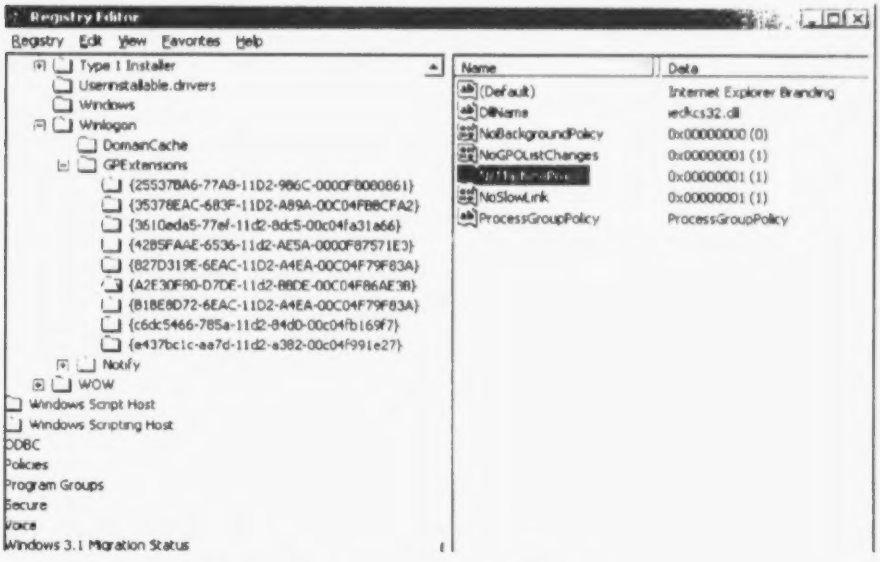

Figure 5: Extensions configuration data

Table 1 gives the meaning of the different values that can be seen in such GPExtensions registry keys.

PS17531.PDF [Page: 28 of 85]

Table 1. Extensions configuration data

VALUE	DATA	DEFAULT	ACTION
DLLName	name		Name of the client-side extension dll if present; otherwise, no dll is necessary
ProcessGroupPolicy	name		Function within the client-side extension to be called when a GPO is passed to the extension
NoMachinePolicy	0 or 1	0 (Process)	If 1, the extension processes a GPO only if it is not a machine GPO
NoUserPolicy	0 or 1	0 (Process)	If 1, the extension processes a GPO only if it is not a user GPO
NoSlowLink	0 or 1	0 (Process)	If 1, the extension processes a GPO only if there is no slow link
NoBackGroundPolicy	0 or 1	0 (Process)	If 1, the extension doesn't process a GPO when a background refresh occurs when a user is logged on the machine
NoGPOListChanges	0 or 1	0 (Process)	If 1, the extension processes the GPO only if there are changes between the cashed GPO information in \Software\Microsoft\Windows\CurrentVersion\Windows\Extensions\<*extension's GUID*>\<x> *in either \HKLM or \HKCU and the information on the computer or user GPO*
PerUserLocalSettings	0 or 1	0 (Disabled)	If disabled, user and computer policies are respectively cached on a per-user and per-machine basis on the registry key: \Software\Microsoft\Windows\CurrentVersion\Group Policy\History\<Client-side extension's GUID >\<a number associated to a policy> in respectively \HKCU and \HKLM If enabled, user policies are cached on a per-user and per-machine basis.
RequiresSuccessfulRegistry	0 or 1	0 (Disabled)	If enabled, the extension must first be a registered COM object to be used
EnabbleAsynchronusProcessing	0 or 1	0 (Sync)	
LastPolicyTime			The last time in minutes when the extension was called. This time is set by the Group Policy engine, not by the client-side extension.

P517531.PDF [Page: 29 of 85]

Three values in the non-volatile configuration data can be modified by policies. These values are NoBackGroundPolicy, NoGPOListChanges, and NoSlowLink. When they are present in a GPO volatile registry key of the form:

\HKLM\Software\Policies\Microsoft\Windows\Group Policy\<Client-side extension's GUID>,

the corresponding client-side extension modifies its configuration data accordingly. Figure 6 shows the contents of such a registry key.

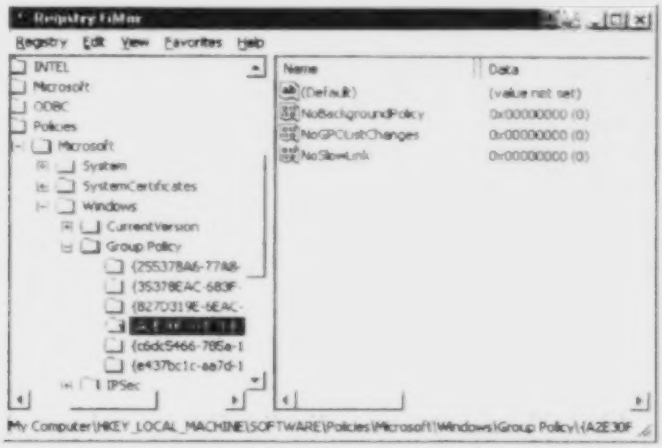

Figure 6: Policies configuration data

4.2 GPO information cached by client-side extensions

For each client-side extension and each GPO processed by an extension, GPO information is cached in the registry. This information gives a summary on the GPO the last time it was processed by the extension.

A GPO is either a user or computer GPO and is composed of components. GPO components are GUID named as GPOs and are associated to a client-side extension. When a GPO is processed by a client-side extension, only components associated to the extension are actually processed by the extension.

For each user or computer GPO corresponds a sequence of characters called a GPO list. A GPO list is a sequence of GPO sublists that are sequences of bracketed GUID enclosed between ([) and (]). In a GPO sublist, the first GUID represents a client-side extension and other GUIDs are GPO's component names that are associated to the client-side extension. The following shows a sample GPO list:

[{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957D-509E-11D1-A7CC-0000F87571E3}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}][{827D319E-

P517531 PDF [Page: 30 of 85]

6EAC-11D2-A4EA-00C04F79F83A}{803E14A0-B4FB-11D0-A0D0-00A0C90F574B}][{B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}].

The first GPO sublist is [{35378EAC-683F-11D2-A89A-00C04FBBCFA2}{0F6B957D-509E-11D1-A7CC-0000F87571E3}{53D6AB1B-2488-11D1-A28C-00C04FB94F17}] where 35378EAC-683F-11D2-A89A-00C04FBBCFA2 is the name of the client-side extension, and 0F6B957D-509E-11D1-A7CC-0000F87571E3 and 53D6AB1B-2488-11D1-A28C-00C04FB94F17 are names of components of the GPO.

When a client-side extension processes a user (computer) GPO, some pieces of GPO information are cached in the following History registry subkey:

\Software\Microsoft\Windows\CurrentVersion\Group Policy\History\<Client-side extension's GUID>\<a number associated to the GPO>

in HKCU (HKLM). As shown in Figure 7, this information contains the GPO list — the data of the "Extensions" value —, the GPO version, and some other pieces of information.

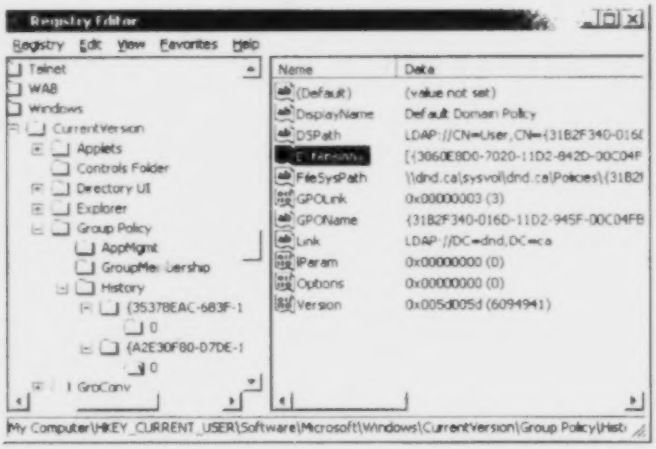

Figure 7: GPO's information cached by a client-side extension

4.3 Extensions processing of GPOs

In this section, we will analyse how GPOs are processed by client-side extensions when the computer boots, users log on to, and policies are refreshed.

At boot, logon, and policy refresh time, the system gets an ordered set of either computer or user GPOs that are applied to the local computer.

At boot time, the system processes computer GPOs . Each client-side extension processes these GPOs from the first to the last only if no one of the conditions (1), (2), and (4) shown below is satisfied.

At logon time, the system processes user GPOs. Each client-side extension processes these GPOs from the first to the last only if no one of the conditions (2), (4), and (5) is satisfied.

At computer refresh time, the system processes computer GPOs. Each client-side extension processes these GPOs from the first to the last only if no one of the conditions (1) to (4) is satisfied.

At user refresh time, the system processes user GPOs. Each client-side extension processes these GPOs from the first to the last only if none of the conditions (2) to (5) is satisfied.

1. If the client-side extension is configured with NoMachinePolicy=1.

2. If the client computer has a slow link to the DC that provides the GPOs and the client-side extension is configured with NoSlowLink =1.

3. If the client computer has a logged on user and the client-side extension is configured with NoBackGroundPolicy=1.

4. If the GPO list and the GPO version are equal to the ones stored in History registry keys, and the client-side extension is configured with NoGPOListChanges=1.

5. If the client-side extension is configured with NoUserPolicy=1.

Note: There is one special client-side extension that provides the volatile configuration data for client-side extensions. This extension must have the following value settings: NoMachinePolicy=0, NoSlowLink=0 — if there is a slow link between any computer in the domain and the DC providing its GPOs —, and NoGPOListChanges=0. If the first two values were not set appropriately, the configuration data for client-side extensions would be static. If NoGPOListChanges were set to 1, the volatile configuration data would be lost forever after the first computer shutdown if no GPO modification is made later.

Note: It is not clear from the Microsoft documentation whether or not all client-side extensions are initialised before they are started. If it is not the case, start states of extensions may be unpredictable because there is one extension that modifies volatile client-side extensions' configuration data. If it is not the case, a solution to that would be to start first the client-side extension that provides the client-side volatile configuration data and, after completion, starts the others.

P517531.PDF [Page: 32 of 85]

5. Microsoft Management Console (MMC)

Administration of a single computer or a network of computers has evolved in many directions. Today both stand-alone and networked system administration have become increasingly complex. Underlying this new technology are multiple administration programs requiring their own user interface. It is not always easy to find the administration program required for a particular application or peripheral. In addition, administration program user interfaces are not customisable to fit the knowledge and skill level of the administrator. All of these issues contribute to a long learning curve or a high frustration level for system administrators.

In summary, computer system and network administrators face these problems:

- Administration tools can be hard to find.
- Each administration tool has its own unique user interface.
- In general, tools cannot be customized to the knowledge or skill level of the intended user.

The goal of Microsoft Management Console (MMC) is to minimise the cost of administering Windows-based computers, and to provide a simple, consistent, and integrated user interface and administration model. One of the strengths of MMC is its ability to support task delegation scenarios.

A Microsoft Management Console (MMC) can be used to create, save, and open administrative tools (called MMC *consoles*) that manage a part of a Windows system. MMC does not perform administrative functions, but hosts tools that do. The primary type of tool that can be added to a console is called a snap-in. Other items include ActiveX controls, links to Web pages, folders, taskpad views, and tasks. MMC provides a multiple-document interface (MDI) in which each window is a view. Each view can contain one or more administrative components that supply the management behaviour. Each administrative component is a *snap-in*.

P517531.PDF [Page: 33 of 85]

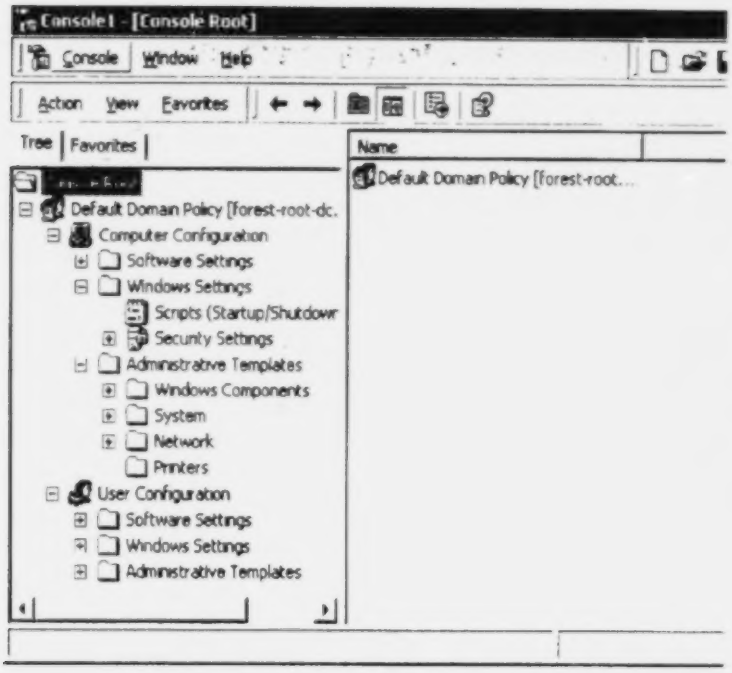

Figure 8: A Group Policy MMC console

Figure 8 shows a MMC console that contains the Group Policy snap-in represented by a tree structure in the left pane. Each branch of the tree is a node. The console tree contains a hierarchy of nodes. Each node is the parent of any node that lies one level below it in the tree hierarchy. Nodes below a parent node are child nodes.

A snap-in is a Component Object Model (COM) in-process server that can be loaded in a MMC process. It is loaded through a dynamic-link library (DLL). The snap-in's COM interface links MMC to the snap-in. MMC does not care how the snap-in communicates with the managed service. Snap-ins can communicate with the managed service through any data protocol that the managed service supports. MMC has no knowledge of the mechanism used for this communication. Both Microsoft developers and independent software vendors (ISVs) can create snap-ins.

A snap-in can be a stand-alone, an extension, or a dual snap-in. Stand-alone and extension snap-ins are respectively snap-ins that can be directly loaded to a console and extend the functions of existing snap-ins. Finally, dual snap-ins are both a stand-alone and an extension snap-ins.

P517531.PDF [Page: 34 of 85]

6. Policies in Group Policy snap-in

Windows 2000 provides a Group Policy snap-in to build GPOs — see Figure 8. As any snap-in, it can be extended by other snap-ins. In this snap-in, policies that apply to computers are in Computer Configuration node while those that apply to users are in User Configuration node.

In this section and subsequent ones, we will study/analyse the current Microsoft policies that can be enabled in a Group Policy snap-in. We will not consider all of them, but only those that are the most important with respect to security.

As seen in Figure 8, both Computer and User Configuration nodes have three child nodes:

- Software Settings — that is the location for ISVs to add further extensions. If no node appears, no nodes have been added by ISVs. No policies are currently defined here.
- Windows Settings — that holds extensions provided by Microsoft. See Section 6.1.
- Administrative Templates — that shows the namespace for some registry-based settings. Adm files create the Administrative Templates namespace as it is done for Windows NT 4.0-based computer. Right-clicking the Administrative Templates node, and then clicking "Add/Remove Templates" can add adm files. See Section 6.2.

6.1 Windows Settings nodes

As shown in Figure 9, a Windows Settings node appears in both Computer Configuration and Users Configuration nodes.

P517531.PDF [Page: 35 of 85]

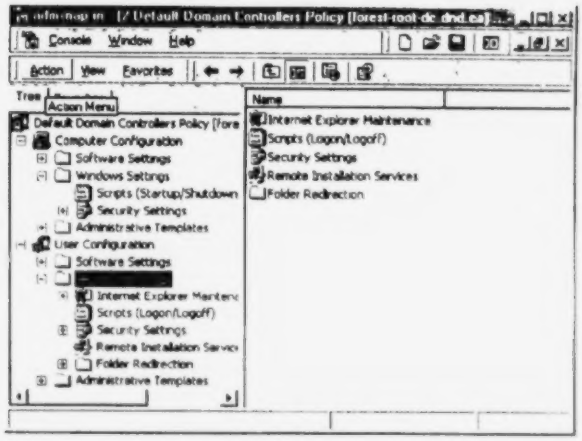

Figure 9: Windows Settings nodes

6.1.1 Windows Settings in Computer Configuration node

The Windows Settings node underneath the Computer Configuration node has two child nodes:

- Scripts (Startup/Shutdow) — that contains script files to be run at computer startup/shutdown.
- Security Settings

The Security Settings node has the following child nodes in which policies are analysed in the subsequent subsections.

- Account Policies
- Local Policies
- Event Log
- Restricted Groups
- Systems Services.
- Registry
- File System
- Public Key Policies
- IP Security Policies

PS17521.PDF [Page: 36 of 85]

6.1.1.1 Policies in Account Policies node

The Account Policies node contains domain-wide policies. So these policies are not considered when they are applied to a site or a OU. The Account Policies node has three child nodes: Password Policy, Account Lockup Policy, and Kerberos Authentication Policy.

In the Password Policy node, we can set policies to specify the password length and the maximum password age, require complex passwords, and prevent users from reusing passwords or simple variations of passwords.

In the Account Lockup Policy node, we can set policies that force users to be locked out after a certain number of failed logon attempts, and specify the time period that accounts are frozen.

In the Kerberos Policy, we can modify the settings shown in Figure 10.

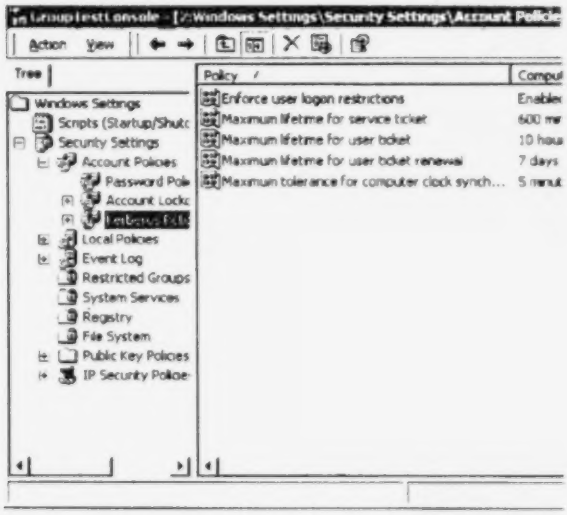

Figure 10: Policies in Accounts Policies node

6.1.1.2 Policies in Local Policies node

The Local Policies node contains three child nodes: Audit Policy, User Rights Assignment and Security Options.

In the Audit Policy node, we can set policies that ask Windows 2000 to record a range of security event types.

P517531.PDF [Page: 37 of 85]

In Users Rights Assignment node, we can set up policies that control the rights assigned to user accounts and security groups for computers. Figure 11 shows some of these settings. By double-clicking on a policy, we can define the policy and then select Security Groups that have the specified right.

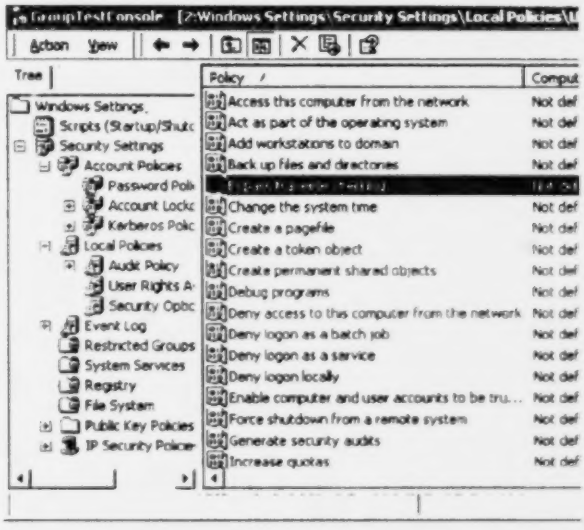

Figure 11: User Rights Assignment

In Security Options node, we can set policies that control a wide variety of security options. Figure 12 shows some of them.

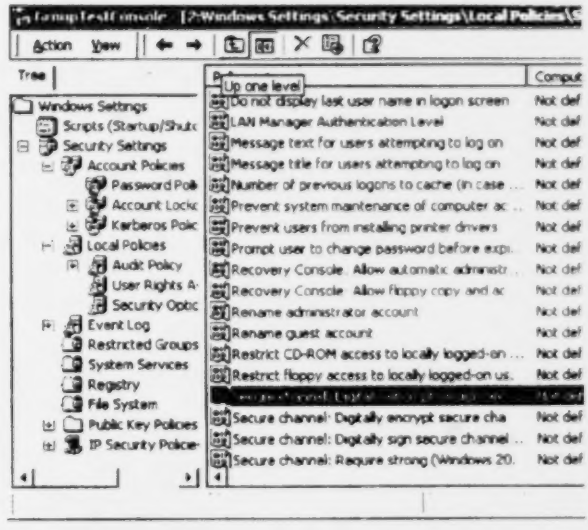
Action View
Tree
Up one level
Windows Settings
Scripts (Startup/Shutc
Security Settings
Account Policies
Password Poli
Account Lockc
Kerberos Polic
Local Policies
Audit Policy
User Rights A
Security Optic
Event Log
Restricted Groups
System Services
Registry
File System
Public Key Policies
IP Security Policie
Do not display last user name in logon screen
LAN Manager Authentication Level
Message text for users attempting to log on
Message title for users attempting to log on
Number of previous logons to cache (in case ...
Prevent system maintenance of computer ac ...
Prevent users from installing printer drivers
Prompt user to change password before expi...
Recovery Console: Allow automatic administr...
Recovery Console: Allow floppy copy and ac...
Rename administrator account
Rename guest account
Restrict CD-ROM access to locally logged-on ...
Restrict floppy access to locally logged-on us...
Secure channel: Digitally encrypt secure cha...
Secure channel: Digitally sign secure channel ...
Secure channel: Require strong (Windows 20...
Not def

Figure 12: Security Options

PS1752[1].PDF [Page: 38 of 85]

6.1.1.3 Policies in Event Log node

We can use policies in the Event Log node to control the settings of the application, system, and security events on computers. For example, we can specify maximum log sizes, how long logged events are maintained, and log retention methods.

6.1.1.4 Policies in Restricted Groups node

Restricted Groups contains security groups that contain members defined centrally. Membership changes for these groups made by local computer administrators are overwritten by those from the Restricted Groups. Using Restricted Groups, we can enforce the membership of these groups by policy and not allow local variations on each computer.

6.1.1.5 Policies in System Services node

System services are user-mode processes that provide services to other user-mode processes. DNS servers, proxy servers, smtp servers, and web servers are example of services. Using System Services policies, we can set the startup mode (manual, automatic, or disabled) of a service, define users rights to manage a service, and define security audit levels.

6.1.1.6 Policies in Registry node

We can use Registry policies to configure security and control security auditing for registry keys and subkeys. Using Registry policies, it is possible to control which users can read or write in the registry. Values of registry keys are not set up here but in the Administrative Templates nodes studied in Sections 6.2, 7, and 8.

6.1.1.7 Policies in File System node

We can use File System policies to configure security for files and folders and control security auditing of files and folders. For example, to make sure that only system administrators can modify system files and folders, we can use File System policies to grant administrators full control over these files and folders and grant read-only permission to other users.

6.1.1.8 Policies in Public Key Policies node

Using Public Key Policies, we can add a new New Data Recovery Agent and set up Automatic Certificate Requests. Also, we can manage lists of trusted Certification Authorities.

Note: The list of Certification Authorities here is associated to computers where the policy is applied or not to a user or a group.

6.1.1.9 Policies in IP Security Policies node

There is only one security policy in the IP Security Policies node. This policy controls the IPSec of the machine. This complex policy is not studied in this work. Further studies need to be conducted on this policy.

6.1.2 Windows Settings in User Configuration node

As shown in Figure 9, the Windows Settings node underneath the Computer Configuration node has the following child nodes:

- Internet Explorer Maintenance — that contains policies described in Section 9.1.
- Scripts (Logon/ Logoff) — that contains policies that set up script files to be run at user logon/logoff
- Security Settings — that contains only one user Public Key Policy.
- Remote Installation Services — that contains a unique policy that sets up the user's control rights on the client installation wizard.
- Folder Redirection — that contains policies redirecting the following user's folders: Application Data, Desktop, My Documents, and Start Menu. A redirected folder can be either on a network share with a UNC pathname or on a local folder.

6.2 Administrative Templates nodes

Policies in Administrative Templates nodes are defined in Administrative Template (adm) files that are used to set registry settings. Two types of registry settings can be defined. The first type is for registry settings contained in the GPO volatile registry keys defined in Section 3.2 while the other one is for registry settings that are either in \HKLM or \HKCU, but are not of the first type. As said previously, type I registry settings are not stored in any hive on the local computer. So, no permanent settings are defined on these registry keys. Type II registry settings are stored in a local computer hive and are called preference settings. If a user modifies such a setting and no policy modifies it later, the setting becomes permanent.

P517531.PDF [Page: 40 of 85]

Note: Windows NT 4.0 registry settings are in fact registry settings of type II. Registry settings of types I and II are respectively displayed in the Group Policy snap-in with blue and red icons.

Administrative Templates policies in the Computer Configuration node are studied in Section 7 while the ones in the User Configuration node are studied in section 8. Furthermore, in Section 10 information on adm files is provided.

P517531.PDF [Page: 41 of 85]

7. Computer Administrative Templates policies

In this section, we will analyse the policies in the Administrative Templates node beneath Computer Configuration node. Figure 13 shows child nodes beneath the Administrative Templates node. In the following three sub-sections, we will respectively analyse policies in the Windows Components, System, and Network components nodes. Because policies in the Printer node are not very important with respect to security, they are not considered herein.

Figure 13: Computer Administratives Templates node

7.1 Policies in Windows Components node

The Windows Components node contain four direct child nodes:

- NetMeeting — that contains only one policy that allows or disallows remote user to share the default desktop object. Usually, processes created by remote users do not belong to the default desktop while processes created by the interactive user belong to the default desktop.
- Internet Explorer — See Section 9.3.
- Task Scheduler — See Section 7.1.1.
- Windows Installer — See Section 7.1.2.

7.1.1 Policies in Task Scheduler node

The Task Scheduler is a service running with the System security token that allows users to schedule tasks to perform. Scheduling a task creates an object that is only accessible by administrators, the system, and the task creator.

The Task Scheduler wizard allows users to create new tasks. To schedule a task from the Task Scheduler wizard a user click successively Start, Control Panel, Tasks Scheduler, and Add Tasks Scheduler. In doing so, a DLL or a COM object is loaded in the User's explorer.exe process. From that, the user can talk to Task Scheduler process (mstask.exe) to schedule new tasks.

Policies in the Task Scheduler node set registry keys that control the initialisation of the DLL or the COM object. By using these policies, it is possible to restrict users access to the service.

Note: The security implemented by these policies is not very secure because a user can creates his own DLL or COM object to access mstask.exe. However, a user can only create scheduled tasks that he can create when the user is logged on. The only difference is the time when the task runs.

Note: Scheduled Task objects are located in %SystemDrive%\%systemroot%\Tasks folder. Only the System has access rights to create objects in this folder. For example, even an administrator cannot paste a Scheduled Task object in this folder.

Policies in Task Scheduler node are shown in the right panel of Figure 13. For all of these policies, if a policy appears both in the Computer and User configuration nodes, the computer policy takes precedence.

The *Hide Property Pages* policy when enabled removes the Properties item from the file menu in Scheduled Tasks and from the context menu that appears when one right-click a task.

The *Prevent Task Run or End* policy when enabled removes the Run and End Task items from the context menu.

The *Disable Drag-and-Drop* policy when enabled disables the Cut, Copy, Paste, and Paste shortcut item on the context menu and the Edit in Scheduled Tasks.

The *Disable New Task Creation* policy when enabled removes the Add Scheduled Task item that starts the New Task Wizard. Also, the system does not respond when users try to move, paste, or drag programs into the Scheduled Tasks folder.

P517531.PDF [Page: 43 of 85]

Note: This policy does not prevent administrators of a computer from using At.exe to create new tasks. This is true because these policies only restrict users' access rights to an interface accessing mstask.exe but not restrict from using other interfaces.

The *Disable Task Deletion* removes when enabled the Delete button in the context menu.

The *Disable Advanced Menu* policy when enabled removes the "Open advanced properties for this task when I click finish" item from the last page of the Scheduled Task wizard.

The *Prohibit Browse* policy removes when enabled the Browse button from Scheduled Task wizard.

7.1.2 Policies in Windows Installer node

Windows Installer is a service running with the System security token that installs software. The security of this service is very important because it can modify system DLLs and registry keys.

The policies in the Windows Installer node are shown in Figure 14.

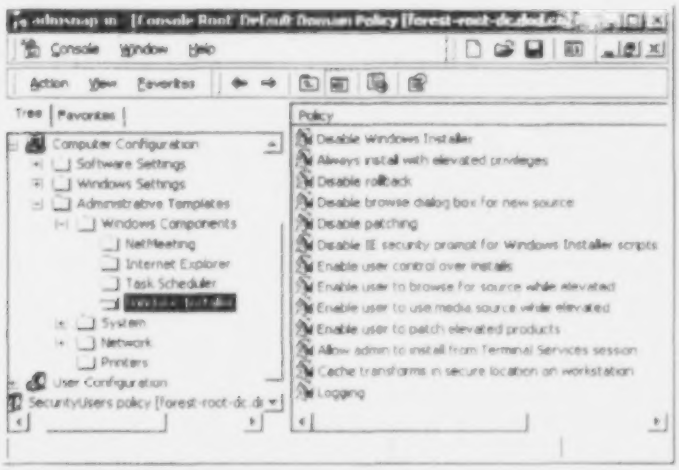

Figure 14: Windows Installer policies

The *Disable Windows Installer* policy when enabled disables or restricts the use of Windows Installer. If the policy is enabled, we can establish an installation policy.

P517531.PDF [Page: 44 of 85]

Security note: In secure Windows 2000-based domains, system administrators that enable this policy should assign a restricted set of programs that users can install through Windows Installer.

The *Always install with elevated privileges* policy when enabled asks Windows Installer to install programs with the System privileges—using the System security token. This policy appears both in Computer Configuration and User Configuration nodes. To make this policy effective, we must enable it in both places.

Security note: This policy should be disabled if possible because a user that installs an application can modify and add files and registry keys that he cannot normally modify or add. If this policy has to be enabled because some applications cannot be installed with normal user privileges, the programs that users can install should be restricted. New Windows 2000 applications need only normal user privileges to be installed.

The *Disable rollback* policy when enabled prohibits Windows Installer from generating the files it needs to reverse an interrupt or unsuccessful installation. This policy appears in Computer and user Configuration nodes. The policy is enabled if it appears in either node. Do not enable this policy if it is not essential, for example to save disk space.

The *Disable browse dialog box for new source* policy when enabled disables the Browse button in the Windows Installer wizard. If this policy is disabled or not configured, the browse button is enabled when an installation is running in the user's security context, but only system administrators can browse when an installation is running with elevated system privileges.

The *Disable patching* policy when enabled prevents users from using Windows Installer to install patches. This policy applies only to installations that run in the user's security context.

The *Disable IE security prompt for Windows Installer scripts* policy when enabled allows Web-based applications to install software on a computer without notifying the user. By default, the system warns users and allows them to select or refuse the installation.

The *Enable user control over installs* policy when enabled permits users to change installation options that are available only to system administrators. This policy is designed for less restrictive environments.

The *Enable user to browse for source while elevated* policy when enabled enables the browse button in the Windows Installer wizard during privileged installations.

PS17531.PDF [Page: 45 of 85]

The *Enable user to use media source while elevated* policy when enabled allows users to install applications from removable media, such as floppy disks and CD-ROMS, during privileged installations.

The *Enable user to patch elevated products* policy when enabled permits all users to install patches.

Security note: This policy should be disabled because only system administrators should install patches.

The *Allow admin to install from Terminal Services session* policy allows Terminal Services administrators to install and configure application remotely. By default this policy is enabled.

The *Cache transforms in secure location on workstation Properties* policy when enabled saves copies of transform files in a secure location on the local computer. Transform files consists of instructions to modify or customize an application during installation. If this policy is enabled, the transform file is saved in a secure location instead of in the user profile. This policy is designated to prevent unauthorised or malicious editing of transform files.

The *Logging* policy when enabled specifies the types of events that Windows Installer records in its transaction log for each installation. The log, Msi.log, appears in the Temp directory of the *%systemroot%* folder.

7.2 Policies in System node

As shown in the Figure 15, the System node contains policies and has the following direct child nodes:

- Logon — See Section 7.2.1.
- Disk Quotas — that contains six policies that configure disk quotas.
- DNS Client — that contains a single policy that sets up the DNS suffix for the affected computers. When this policy is enabled, other suffixes entered by administrators in different dialog boxes are ignored.
- Group Policy — that is a very important node where policies are analysed in Section 7.2.2.
- Windows File Protection — that contains four policies configuring the Windows File Protection service.

P517531.PDF [Page: 46 of 85]

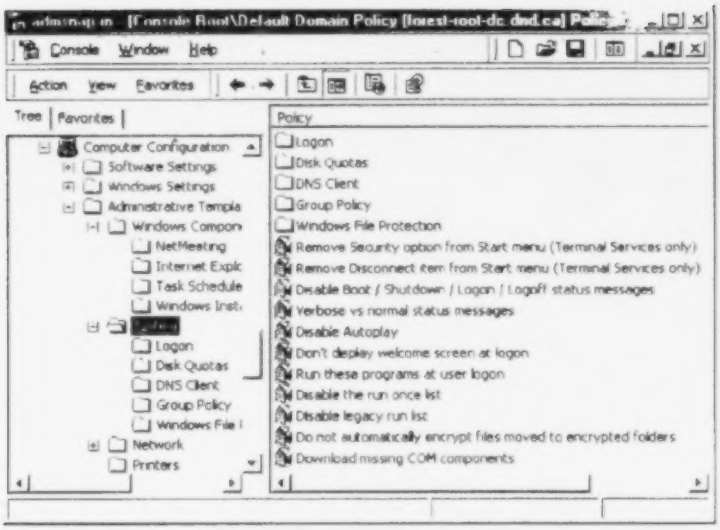

Figure 15: Nodes and policies in System node

Policies in the System node are self-explanatory and are not very important in general with respect to security. Two of them are worth more comments.

The *Run these programs at user logon* policy when enabled allows system administrators to set applications to be run at logon time.

The *Download missing Com components* policy when enabled asks the system to search needed COM objects not present on the local computer in the Active Directory. If they are found, these objects are downloaded.

Note: What happens in general when a COM object is needed but cannot be found?

7.2.1 Policies in Logon node

The policies in Logon node are shown in Figure 16. These policies control the processing of logon and start-up scripts and the loading of roaming profiles. We analyse here only the most important policies.

The *Do not detect slow network connections* policy when enabled asks the system to not detect slow connections or recognise a connection as being slow. As a result, other policies that are related to slow connections are ignored.

Security note: This later policy should not be applied if possible.

The *Slow network connection for timeout for user profiles* policy when enabled defines a slow connection for roaming user profiles.

P517531.PDF [Page: 47 of 85]

The *Log users off when roaming profile fails policy* when enabled asks the system to log a user off automatically when the system cannot load the user's roaming user profile. Using this policy, it is possible to make mandatory profiles from simple profiles.

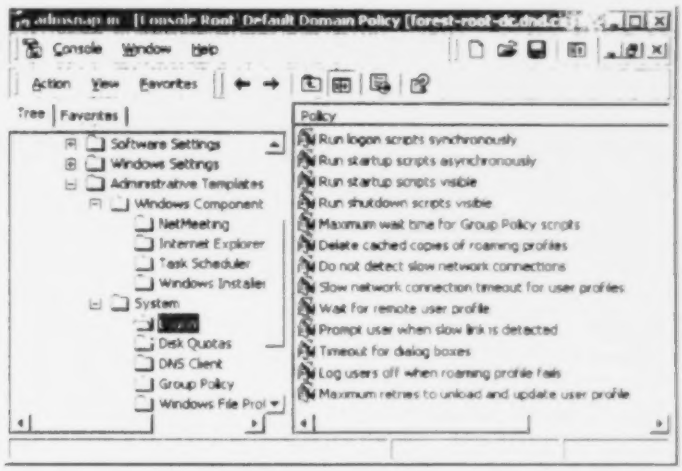

Figure 16: Logon policies in System node

7.2.2 Policies in Group Policy node

Policies in this node are shown in Figure 17 and are very important with respect to security.

P517531.PDF [Page: 48 of 85]

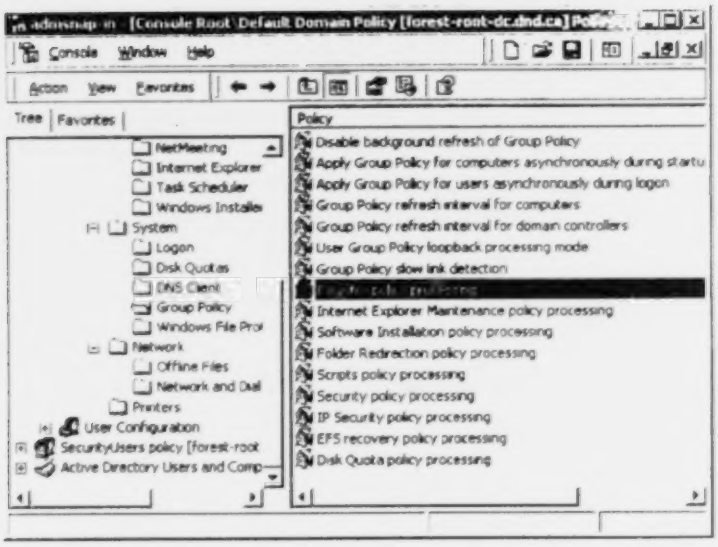

Figure 17: Group Policies policies in System node

The last nine policies are policies that control how policies are reapplied or refreshed. For each of these policies when enabled, a user can select or not the same three sub-policies –some sub-policies though are not displayed for some of these policies because they are fixed by the client-side extension. Figure 18 shows the three sub-policies for the *Internet Explorer Maintenance policy processing* policy.

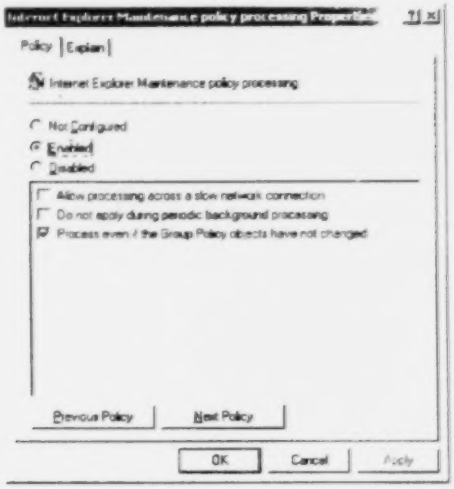

Figure 18: Refresh sub-policies for Group Policy policies

If "Allow processing across a slow network connection" is selected, the client-side extension to which the policy applies processes the GPOs even

P517531.PDF [Page: 49 of 85]

though the computer has a slow link with the domain controller that provides them.

If "Do not apply during periodic background processing" is not selected, the client-side extension to which the policy applies is called at periodic refresh time. This sub-policy is used to modify the default behaviour of client-side extensions.

If "Process even if the Group Policy objects is not changed" is selected, the client-side extension to which the policy applies processes the GPOs when called even though the policy has not been modified. This sub-policy is used to modify the default behaviour of client-side extensions that processes GPOs only when they are modified. This sub-policy is used to enforce settings that could have been modified by users.

Security note: If users can modify settings set up by a client-side extension and system administrators want to enforce these settings, the administrators must deselect the second sub-policy and select the others.

Client-side extensions process GPOs and are configured through registry values — see Section 4. Each of the nine last policies in the Group Policy node provides the volatile configuration data for a client-side extension. The *Registry policy processing* policy controls the volatile configuration data for the client-side extension that defines the volatile configuration data for all client-side extensions. For each of the nine policies, Table 2 shows the action on GPOs taken by their corresponding client-side extension and the GUIDs of these extensions. Extensions' names are also shown in Figure 5.

P517531.PDF [Page: 50 of 85]

Table 2. Names and actions of client-side extensions

Policy and name of the associated client-side extension	**Action made by the associated client-side extension**
Registry policy processing Extension's name= 35378EAC-683F-11D2-A89A-00C04FBBCFA2	Copy in the registry the values in the GPOs' Registry.pol files. This extension writes in the registry the volatile configuration data of client-side extensions.
Internet Explorer Maintenance policy processing A2E30F80-D7DE-11D2-BBDE-00C04F86AE3B	Process GPOs' policies set in the Windows Settings\Internet Explorer Maintenance node
Software Installation policy processing C6DC5466-785A-11D2-84D0-00C04FB169F7	Process GPOs' policies set in the Software Settings\Software Installation node
Folder Redirection policy processing 25537BA6-77A8-11D2-9B6C-0000F8080861	Process GPOs policies set in the Windows Setting\Folder Redirection node
Scripts policy processing 42B5FAAE-6536-11D2-AE5A-0000F87571E3	Process GPOs' scripts in both Windows Settings\Scripts (Startup/Shutdown) and (Logon/Logoff) nodes
Security policy processing 827D319E-6EAC-11D2-A4EA-00C04F79F83A	Process GPOs' policies set in the Security Settings node (minus the nodes shown in the next three policies)
IP Security policy processing E437BC1C-AAD7-11D2-00C04F99E27	Process GPOs' policies set in the Security Settings\IP Security Policies on Active Directory node
EFS recovery policy processing B1BE8D72-6EAC-11D2-A4EA-00C04F79F83A	Process GPOs' encryption policies set in the Windows Settings\Security Settings node
Disk Quota policy processing 3610EDA5-77EF-11D2-8DC5-00C04FA31A66	Process GPOs' policies set in Computer Configuration\Administratives Templates\System\File System\Disk Quota node

P517531.PDF [Page: 51 of 85]

Note: Theoretically, it would be possible that a policy in a GPO be processed by more than one client-side extension because all client-side extensions work independently on the same GPOs.

Now, let us consider the other policies in the Group Policy node.

The *Disable background refresh of Group Policy* policy when enabled disables GPO processing when a user is logged on. So, no client-side extensions are called when a user is logged on. When this policy is enabled, the value *NoBkGndGroupPolicy=1* is set in the volatile registry key: \HKLM\Software\Microsoft\CurrentVersion\Windows\Policies\system. The system reads this value to determine whether or not it loads the GPOs when a user is logged on.

Security note: It is better to not enable this policy because a user can be logged on for a very long period. No policy refreshing would occur during this time interval.

The *Apply Group Policy for computers asynchronously during startup* policy when enabled asks the system to start client-side extensions asynchronously.

The *Apply Group Policy for users asynchronously during logon* policies when enabled determine if client-side extensions terminate before the user can use the computer.

The *Group Policy refresh interval for computer* and *the Group policy for domain controllers* policies when enabled define respectively the refresh time interval for the computer's GPO processing and the user's GPO processing.

The *User Group Policy loopback processing* policy when enabled determines if user policies are considered or not. Using that it is possible to apply only computer policies to a machine.

The *Group Policy slow link detection* policy when enabled defines what is a slow link. . This policy defines slow connection for policies in Computer Configuration node.

7.3 Policies in Network node

The Network node contains the following two child nodes:

- Offlines files — that contains 17 policies related to offline file processing. These policies are not considered herein.

P517531.PDF [Page: 52 of 85]

- Network and Dial-up Connections — that contains a single policy that is analysed just below.

The *Prohibit configuration of connection sharing policy* when enabled prohibits administrators to configure their computer as an Internet gateway for a small network. Internet connection sharing is designated to provide a single step of configuration on a computer to provide a translated connection to the Internet.

P517531.PDF [Page: 53 of 85]

8. User Administrative Templates policies

In this section we will study/analyse the policies in the Administrative Templates node in User Configuration node. Figure 19 shows child nodes beneath the Administrative Templates node. Much of the policies included in this Administrative Template node are policies that configure the user's environment. So, the set of policies that are important with respect to the security is less important than the one studied in Section 7. In the following six sub-sections, we will respectively analyse policies in the Windows Components, Start Menu & Taskbar, Desktop, Control Panel, Network, System, and Network components child nodes.

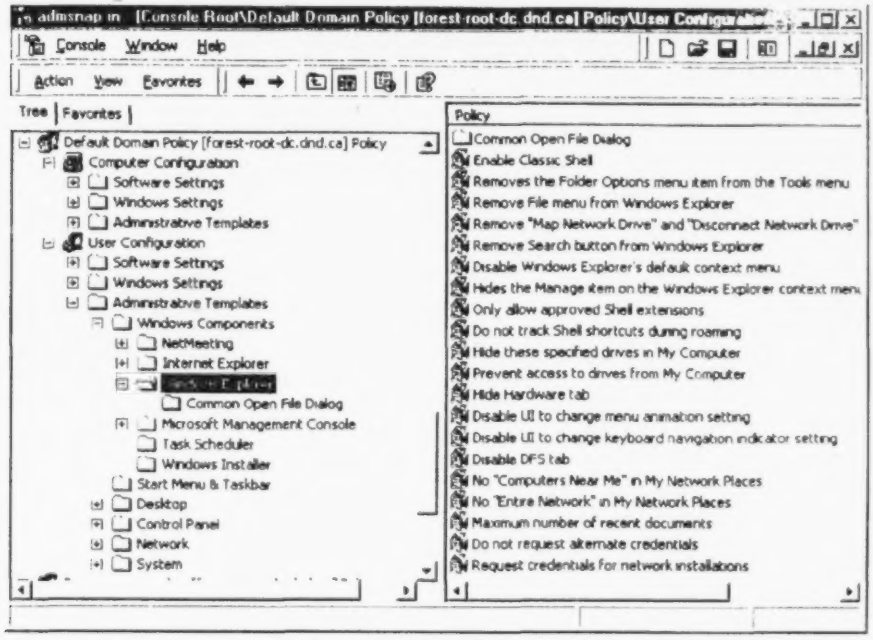
Console Window Help
Action View Favorites
Tree Favorites
Default Domain Policy [forest-root-dc.dnd.ca] Policy
Computer Configuration
Software Settings
Windows Settings
Administrative Templates
User Configuration
Software Settings
Windows Settings
Administrative Templates
Windows Components
NetMeeting
Internet Explorer
Common Open File Dialog
Microsoft Management Console
Task Scheduler
Windows Installer
Start Menu & Taskbar
Desktop
Control Panel
Network
System
Policy
Common Open File Dialog
Enable Classic Shell
Removes the Folder Options menu item from the Tools menu
Remove File menu from Windows Explorer
Remove "Map Network Drive" and "Disconnect Network Drive"
Remove Search button from Windows Explorer
Disable Windows Explorer's default context menu
Hides the Manage item on the Windows Explorer context menu
Only allow approved Shell extensions
Do not track Shell shortcuts during roaming
Hide these specified drives in My Computer
Prevent access to drives from My Computer
Hide Hardware tab
Disable UI to change menu animation setting
Disable UI to change keyboard navigation indicator setting
Disable DFS tab
No "Computers Near Me" in My Network Places
No "Entire Network" in My Network Places
Maximum number of recent documents
Do not request alternate credentials
Request credentials for network installations

Figure 19: The User Administrative Templates node

8.1 Policies in Windows Components node

The Windows Components node contain six direct child nodes:

- NetMeeting — that contains NetMeeting policies. NetMeeting is outside the scope of this work.
- Internet Explorer — that contains policies described in Section 9.2.

P517531.PDF [Page: 54 of 85]

- Windows Explorer — that contains policies shown in the left panel of Figure 19. These settings control the user's view of Explorer.

- Microsoft Management Console — that contains policies described in Section 8.1.1.

- Task Scheduler — that contains policies that are similar to those studied in Section 7. If such a policy is defined and configured in both Computer Configuration and User Configuration node, the setting in Computer Configuration takes precedence.

- Windows Installer — that contains policies described in Section 8.1.2.

8.1.1 Policies in Microsoft Management Console node

As shown in Figure 20, the Microsoft Management Console node contains two policies and a unique child node that contains two nodes.

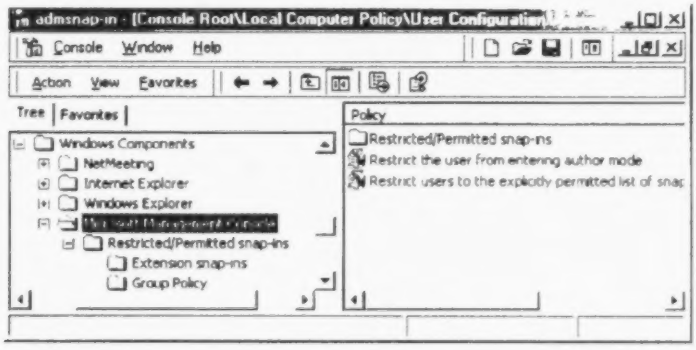

Figure 20: Policies in the MMC node

The *Restrict the user from entering author mode* policy when enabled prevents system administrators to open the MMC in author mode.

The *Restrict users to the explicit list of snap-ins* policy when enabled allows users to access a snap-in only if the snap-in is enabled in the Restricted/Permitted snap-in node. Hence, users cannot access snap-ins that are not configured. If this policy is disabled, system administrators can access snap-ins that are not configured.

P517531.PDF [Page: 55 of 85]

8.1.1.1 Policies in Permitted/Restricted Snap-ins node

Figure 21 shows the policies in the Permitted/Restricted Snap-ins node. For each policy in this node corresponds a snap-in. If the policy is enabled, system administrators can see the snap-in.

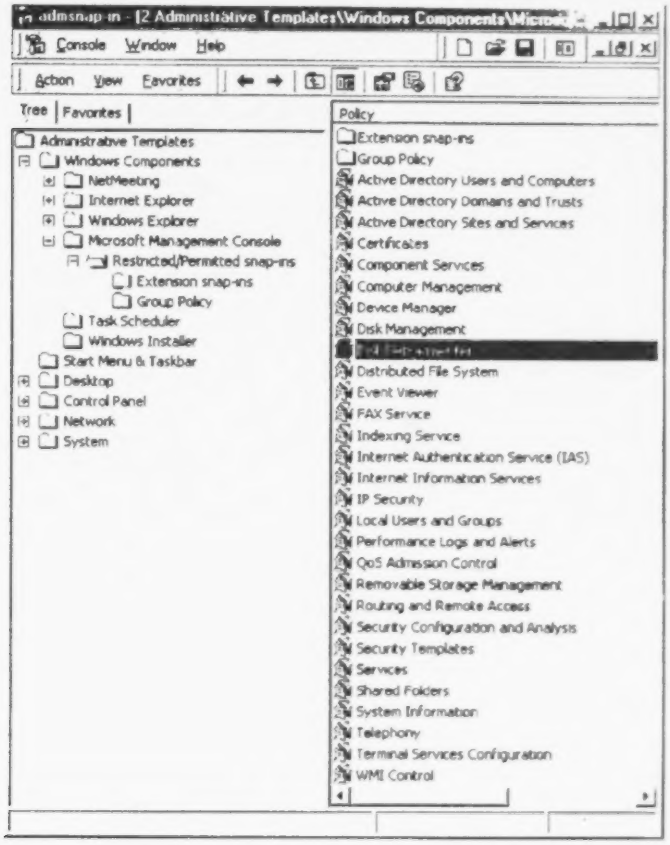

Figure 21: Policies in the Permitted/Restricted Snap-ins node

8.1.1.2 Policies in Extension Snap-ins node

Figure 22 shows the policies in Extension Snap-ins node. For each policy in this node corresponds an extension snap-in. If the policy is enabled, system administrators can see the extension.

P5175S1.PDF [Page: 56 of 85]

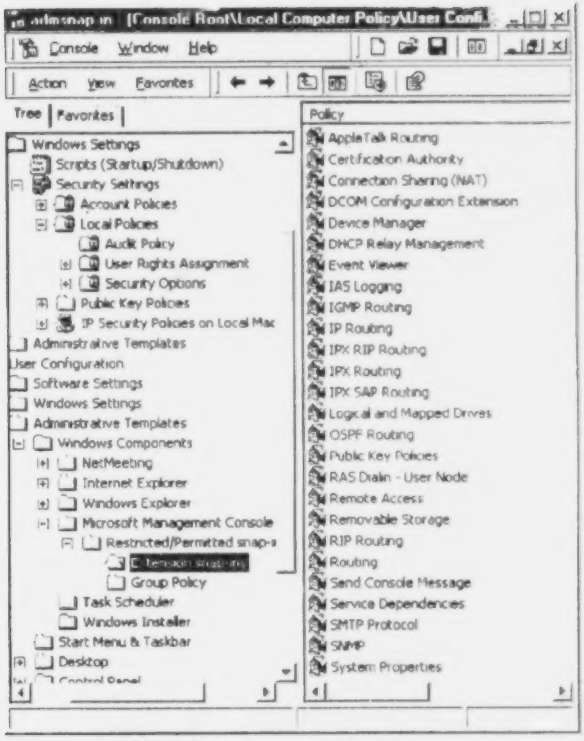

Figure 22: Policies in the Extension Snap-ins node

8.1.1.3 Policies in Group Policy node

Figure 23 shows the policies in the Group Policy node. For each snap-in the Group Policy snap-in corresponds a policy. If the policy is enabled, system administrators can see the corresponding snap-in in the Group Policy snap-in.

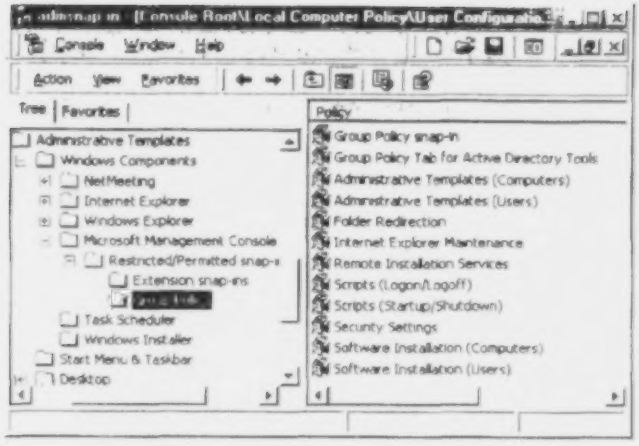

Figure 23: Policies in the Group Policy node

8.1.2 Policies in Windows Installer node

As stated in Section 7.1.2, Windows Installer is a service running with the System security token that installs software. The security of this service is very important because it can modify system DLLs and registry keys.

The policies in Windows Installer node are shown in Figure 24.

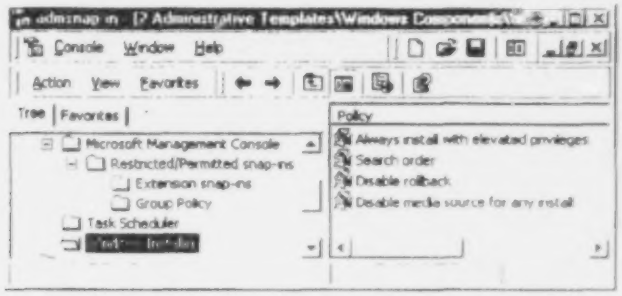

Figure 24: Policies in the Windows Installer node

The first and the third policies are also in Windows Installer node in Computer Configuration node. To be effective, the *Always install with elevated privileges* policy must be enabled in both Computer and User Configuration nodes while the *Disable Rollback* policy must be enabled in either one.

Security note: If the Always Install with elevated privilege is enabled in both Computer and User Configuration nodes, all installations are made under the system's security context. This is very dangerous. For example, a skilled user could create a program that modifies his privileges stored in the Active

Directory. Therefore, if this policy is enabled, the set of applications that can be installed by users must be specified by another policy and be trusted.

The *Search Order* policy when enabled specifies the order in which Windows Installer searches for installation files.

The *Disable media source for any install* policy when enabled disallows the user to install any application from removable media even though the installation is made in the user's security context. If this policy is disabled or not configured, only system administrators can install from removable media when the installation doesn't run in the user's security context.

8.2 Policies in Start Menu & Taskbar node

Figure 25 shows the policies in Start Menu &Taskbar node.

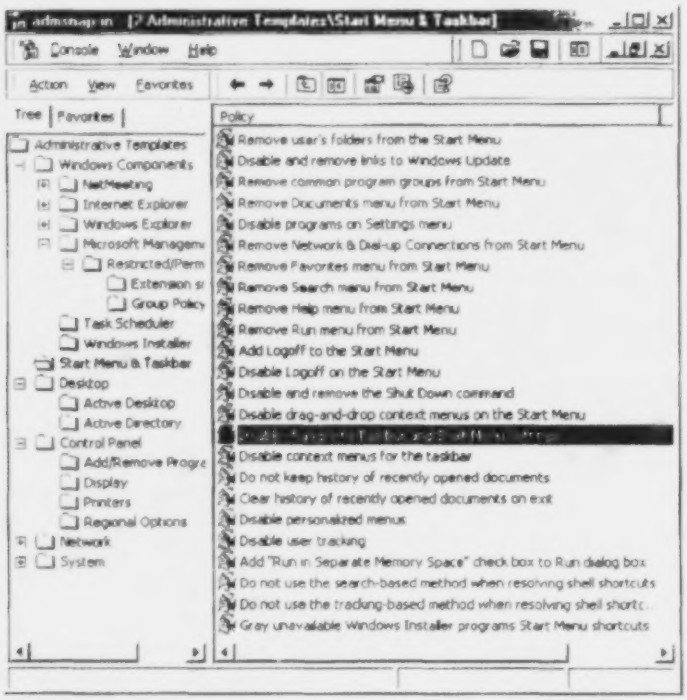
Console Window Help
Action View Favorites
Tree Favorites
Policy
Administrative Templates
Windows Components
NetMeeting
Internet Explorer
Windows Explorer
Task Scheduler
Windows Installer
Start Menu & Taskbar
Desktop
Active Desktop
Active Directory
Control Panel
Display
Printers
Regional Options
Network
System
Remove user's folders from the Start Menu
Disable and remove links to Windows Update
Remove common program groups from Start Menu
Remove Documents menu from Start Menu
Disable programs on Settings menu
Remove Network & Dial-up Connections from Start Menu
Remove Favorites menu from Start Menu
Remove Search menu from Start Menu
Remove Help menu from Start Menu
Remove Run menu from Start Menu
Add Logoff to the Start Menu
Disable Logoff on the Start Menu
Disable and remove the Shut Down command
Disable drag-and-drop context menus on the Start Menu
Disable context menus for the taskbar
Do not keep history of recently opened documents
Clear history of recently opened documents on exit
Disable personalized menus
Disable user tracking
Add "Run in Separate Memory Space" check box to Run dialog box
Do not use the search-based method when resolving shell shortcuts
Gray unavailable Windows Installer programs Start Menu shortcuts

Figure 25: Policies in the Sart Menu & Taskbar node.

Using these policies it is possible to customize the user's interface to objects on the Taskbar. Hence, it is possible to restrict/allow the user's access to some menus accessible after either a click on the Start button or a right-click on an object located on the Taskbar.

Even though these policies are not very important with respect to security because users could access the same objects though other interfaces, we analyse here two of these policies.

The *Disable changes to Taskbar and Start Menu Settings* policy when enabled removes the "Taskbar & Start Menu" item from the "Settings" menu on the "Start" menu. By clicking on the "Taskbar & Start Menu" item, users access the dialog box shown in Figure 26 to customize some menus accessible from the "Start" button.

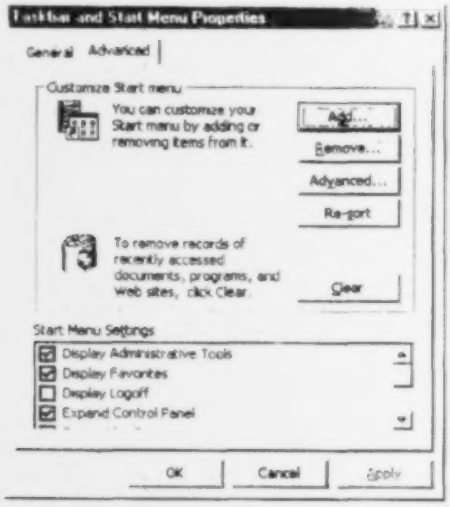

Figure 26: Start button customisation dialog box

The *Disable context menus for the taskbar* policy when enabled hides the menus that appear when users right-click the taskbar and items on the taskbar, such as the Start button, the clock, and the taskbar buttons.

8.3 Policies in Desktop node

Figure 27 shows the policies in the Desktop node.

P517531.PDF [Page: 60 of 85]

Console Window Help
Action View Favorites
Tree Favorites
Policy
Active Desktop
Active Directory
Hide all icons on Desktop
Remove My Documents icon from desktop
Remove My Documents icon from Start Menu
Hide My Network Places icon on desktop
Hide Internet Explorer icon on desktop
Do not add shares of recently opened documents to My Network
Prohibit user from changing My Documents path
Disable adding, dragging, dropping and closing the Taskbar's tool
Disable adjusting desktop toolbars
Don't save settings at exit
Windows Components
Control Panel
Network
System

Figure 27: Policies in the Desktop node

Using these policies it is possible to customize the user's interface to objects on the desktop. These policies are not important with respect to security.

8.4 Policies in Control Panel node

As shown in Figure 28, the Control Panel node contains three policies and four child nodes.

The *Disable Control Panel* policy when enabled prevents Control.exe, the program file for Control Panel, from starting. This policy removes also the "Control Panel " item on the Start menu. Moreover, if users try to select a Control Panel item from the Properties item on a context menu, a message explains that a policy prevents the action.

The *Hide specified Control Panel items and folders* policy when enabled removes Control Panel items such as Display and folders from the Control Panel window and the Start menu. To hide a Control Panel item, write the cpl file corresponding to the item. To hide a folder, type the folder name.

The *Show only specified control panel applets* policy when enabled hides all Control Panel items and folders except those specified in the policy.

PS17531.PDF [Page: 61 of 85]

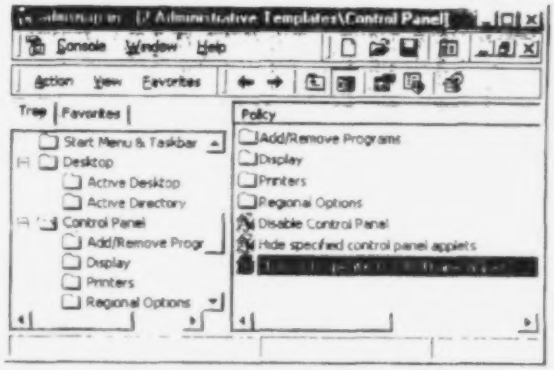

Figure 28: Policies in the Control Panel node

Policies in the first, second, and fourth nodes control the user's view of respectively the "Add/Remove", "Display", and "Regional Options" dialog boxes obtained from the "Control Panel" menu or window. Finally, the Printers node contains policies on printers.

8.5 Policies in Network node

The Network node contains the following two child nodes:

- Offlines files — that contains 12 policies related to offline file processing. These policies are not considered here.
- Network and Dial-up Connections — that contains the policies shown in Fig. 29.

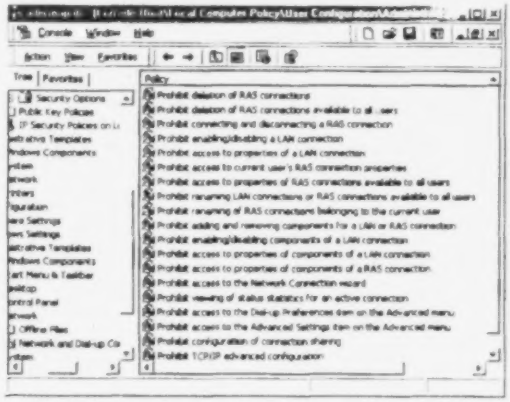

Figure 29: Policies in the Network and Dial-up Connections node

Policies in the Network and Dial-up Connections node control the user's view of some of the dialog boxes accessible by clicking icons in the window shown in Figure 30.

P517531.PDF [Page: 62 of 85]

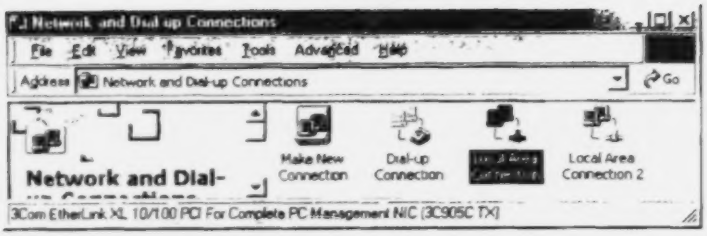
Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Address Network and Dial-up Connections
Go
Network and Dial-
Make New Connection
Dial-up Connection
Local Area Connection 2
3Com EtherLink XL 10/100 PCI For Complete PC Management NIC (3C905C-TX)

Figure 30: The Network and Dial-up Connections window

For example, by right-clicking Local Area Connection and then Properties, the dialog box shown in Figure 31 appears.

The *Prohibit access to Properties of a LAN connection* policy when enabled prohibits access to this dialog box.

The *Prohibit access to properties of components of a LAN connection* policy when enabled disables the Properties button of this dialog box.

The *Prohibit TCP/IP advanced configuration* policy when enabled disables the advanced button on the dialog box shown in Figure 32. This later dialog box can be accessed by double-clicking on "Internet Protocol (TCP/IP)" in the dialog box shown in Figure 31.

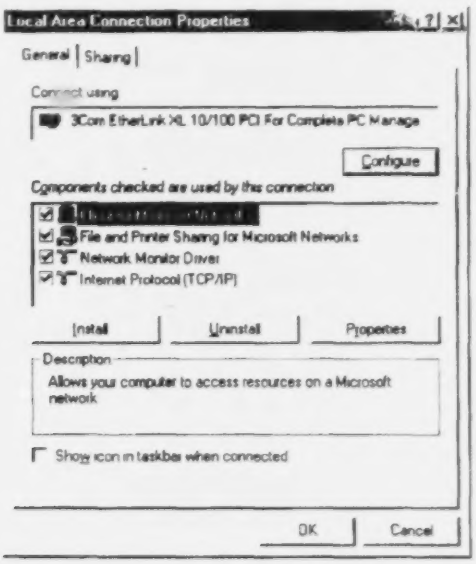

Figure 31: Local Area Connection Properties dialog box

P517531.PDF [Page: 63 of 85]

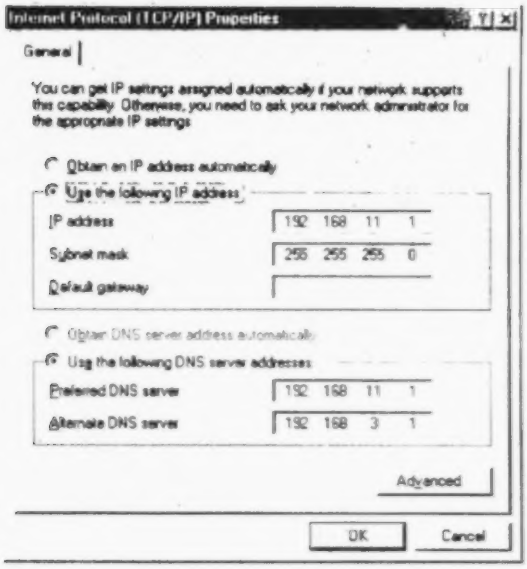
Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address
192 168 11 1
Subnet mask
255 255 255 0
Default gateway
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server
192 168 11 1
Alternate DNS server
192 168 3 1
Advanced
OK
Cancel

Figure 32: Advanced button

8.6 Policies in System node

As shown in the Figure 33, the System node contains policies and has two direct child nodes:

- Logon/Logoff– See Section 8.6.1.
- Group Policy – that is a very important node analysed in Section 8.6.2.

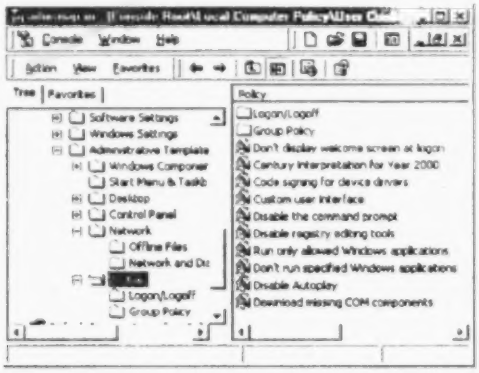

Figure 33: Nodes and policies in System node

We discuss here policies in the System node that are important with respect to security and are not self-explanatory.

P517531.PDF [Page: 64 of 85]

The *Code signing for device driver* policy when enabled allows system administrators to set up the system behaviour when the user imports a new driver. The system can ignore the code signing, ask the user or block the driver installation.

Security note: In a secure environment, code signing should be mandatory.

The *Custom user interface* policy when enabled allows system administrators to replace Explorer.exe by another program. This program can be on the local machine or a network share.

The *Run only allowed Windows applications* policy when enabled allows system administrators to define the set of applications that a user can run.

Security Note: In a secure environment, this policy should be used to prevent users from running Trojan horses and non-secure applications.

Download missing Com components policy when enabled asks the system to search needed COM objects not present on the local computer in the Active Directory. If they are found, these objects are downloaded. This policy appears also in Computer Config[illegible]on node. This later prevails on the one here.

8.6.1 Policies in Logon node

The policies in the Logon node are shown in Figure 34.

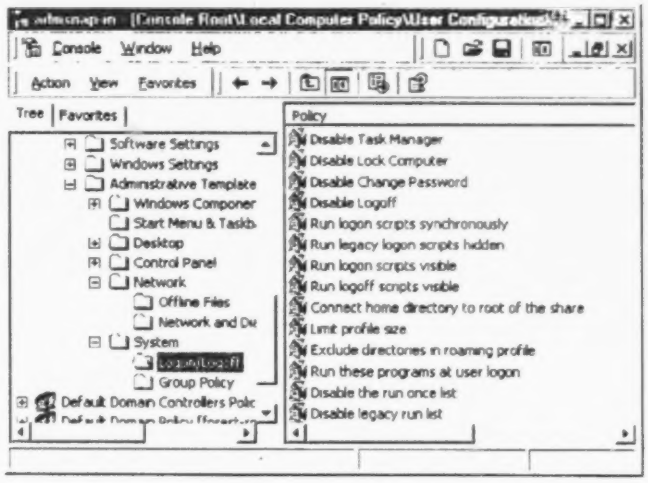

Figure 34: Policies in the Logon node

We analyse here only the most important policies.

PS17531.PDF [Page: 65 of 85]

The *Run this program at user logon* policy when enabled specifies additional programs or documents that Windows starts automatically when users logs on to the system.

The *Disable the run once list* policy when enabled asks the system to ignore the run-once list. The run-once list is the standard list of programs that the system starts when a user logs on to a system. The same setting in the Computer Configuration node takes precedence over this setting.

The *Disable legacy run list* policy when enabled asks the system to ignore the legacy run list. The legacy run list is a list of programs that the system starts when a user logs on to a system. The same setting in the Computer Configuration node takes precedence over this setting.

8.6.2 Policies in Group Policy node

Policies in the Group policy node are shown in Figure 35.

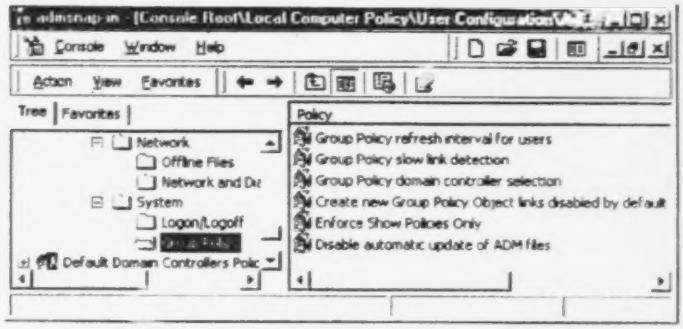

Figure 35: Policies in the Group Policy node

Three of these policies are related to security.

The Group Policy refresh interval for users defines the refresh time interval between two successive GPO processing.

The *Group Policy slow link detection* policy defines what is a slow link. This policy defines slow connection for policies in User Configuration node.

The *Group policy domain controller selection* policy defines from which domain controller the GPOs are imported.

P517531.PDF [Page: 66 of 85]

9. Internet Explorer 5.x security settings

Internet Explorer and Netscape Navigator are two very important applications that need secure configurations. In this section, we analyse the Group Policy policies that applies to IE 5.x.

IE 5.x security settings are either user settings or computer settings. As shown in Figure 36, user settings are both in User Configuration/Windows Settings/Internet Explorer Maintenance and in User Configuration/Administrative Templates /Windows Components/Internet Explorer nodes while computer settings are in Computer Configuration/Administrative Templates/Windows Components/Internet Explorer node.

Figure 36: User and computer settings for IE

9.1 User settings in Windows Settings node

As shown in the right pane of the Figure 36, the Internet Explorer Maintenance node has the following child nodes:

- Browser User Interface — that contains browser settings for title and background, animated bitmaps, customs logos, toolbar buttons

- Connection — See Section 9.1.2.
- URLs — that contains URLs for Favourites and Links, home page, search page, and online help page. Also, it contains settings on channels.
- Security — See Section 9.1.3.
- Programs — that contains a unique policy that determines which program Windows automatically uses for each of the following Internet services: HTML editor, E-mail, Newsgroups, Internet call, Calendar, and Contact list.

Before describing the policies in Connection and Security nodes, we describe briefly what is a connection.

9.1.1 Browser connections

A browser connection is either a dial-up connection or a LAN connection. A user may have multiple dial-up connections but only one LAN connection can be configured from an IE 5.x browser. Only LAN connections are described here. Figures 37 and 38 show the information included in a sample LAN connection.

If Automatic detect settings is selected in Figure 37, the detection of the browser settings is enabled for DHCP and DNS. However, DHCP servers or DNS servers or both have to be configured. For enabling automatic detection on a DNS, we need to configure either a host record or CNAME record in the DNS database file. If the host record is used, we enter a host record named wpad that points to the IP address of the Web server that contains the pac, jvs, js, or ins configuration file. Internet Explorer constructs a URL based on the host name wpad and the computer's DNS domain. If the domain is domain.com for example, the browser uses the following pathname to get the configuration file: http://wpad.domain.com/wpad.dat. Therefore, on the Web server wpad, we must set up a file or a redirection point named wpad.dat, which delivers the contents of the automatic configuration file.

If "Use automatic configuration script" is selected, the address field contains the address of an .ins configuration file, which defines IE options and some standard proxy settings. If the Advanced button is selected, a second URL pointing to a js, jvs, or pac file can be used to configure advanced proxy addresses.

If "Use a proxy server" is selected and then the corresponding Advanced button is clicked, the Window shown in Figure 38 appears, which contains proxy settings.

P517531.PDF [Page: 68 of 85]

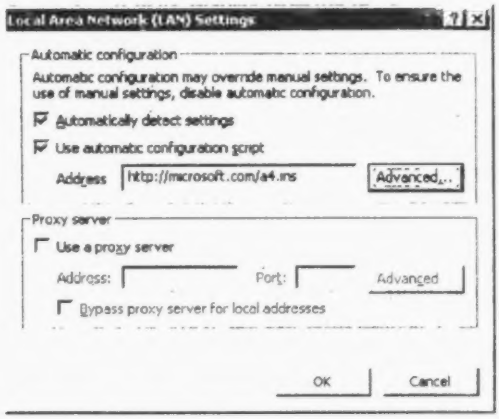

Figure 37: Internet Explorer's LAN Settings page

Figure 38: Proxy Settings from the Advanced button

For each IE 5.x connection corresponds an entry in the following registry key:

\HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Setting\Connections

called here the connection registry key. When a browser starts, it gets its connection information from the default connection entry. If the connection is not possible, the user can only browse the local computer or modify his default connection settings if he is allowed. Moreover, each time a new browser connection is requested, it gets again the registry information to set the connection.

9.1.2 Policies in Connection node

The Connection node contains the following policies:

- Connections Settings
- Automatic Browser Configuration
- Proxy Settings
- User Agent String

The first three policies set up the connection information in the connection registry key while the fourth one sets a text string that can be used to identify the computer.

When the *Connection Settings* policy is enabled and applied, the DefaultConnectionSettings value in the connection registry key is loaded from a domain controller.

The *Automatic Browser Configuration* policy overwrites the settings of the *Connection Settings* policy, but only the connection information that is related to the upper half of Figure 37 is modified.

The *Proxy Settings* policy when enabled overwrites the settings of the *Connection Settings* policy, but only a part of the connection information that is related to the lower half of Figure 37 is modified.

Note: Using current policies in Group Policy, it is not possible to force IE to use connection settings in:

\HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Setting\Connections.

Moreover, it is not clear when this registry key is useful.

9.1.3 Policies in Security node

This node contains two policies and both are important with respect to security.

When the *Security Zones and Content Ratings* policies is enabled, the user's zone settings defined on the domain controller are copied to the following two registry keys:

PS17531.PDF [Page: 70 of 85]

\HKLM\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones and \HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones.

The *Authenticode Settings* policy is used to designate software publishers and credentials agencies as trustworthy.

9.2 User settings in Administrative Templates node

The right pane of Figure 39 shows child nodes and policies in \User Configuration\Administrative Templates\Internet Explorer node.

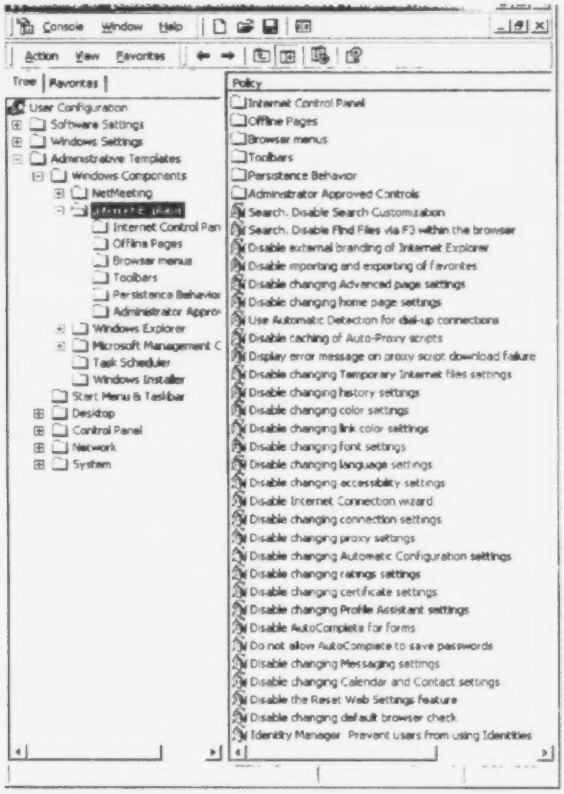

Figure 39: Administrative Templates\Internet Explorer node

Using the policies beneath the Internet Explorer node, it is possible to control what can be seen and modified from the Internet Options dialog box in IE.

9.2.1 Policies in Internet Control Panel node

Internet Control Panel policies control users' access rights to the Internet Options dialog box shown in Figure 40. To get this dialog box from an IE 5.x browser, click the Tools menu and then click Internet Options.

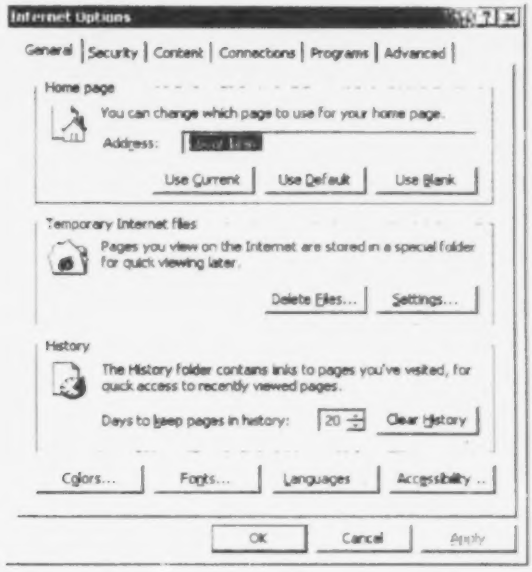

Figure 40: Internet Options dialog box

As shown in the right panel of Figure 41, for each tab in the dialog box above corresponds a policy in Internet Control Panel node. If a policy is disabled or not configured, users can see and change the tab settings—if no other policies deny access to them. If the policy is enabled, users cannot change the settings because the tab is removed from the interface.

Note: These policies control only users access rights to the Internet Options dialog box. Therefore, these policies can be easily circumvented if users can modify settings otherwise. For example, the zone settings in the security tab is written in a registry key that can be modified by users if the Use only machine Settings is disabled . Therefore, the policy denying access to the security tab is not efficient if no registry key policy restricts access to it.

P517531.PDF [Page: 72 of 85]

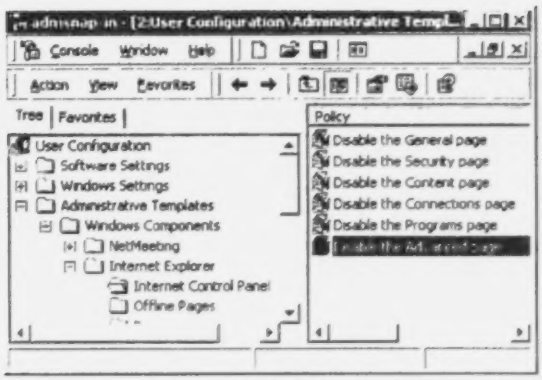

Figure 41: Internet Control Panel policies

9.2.2 Policies in Internet Explorer node

There are thirty Internet Explorer policies shown in Figure 39. Twenty-three of them are policies that disable access to some buttons in tabs shown in Figure 40. These later policies are meaningful only if users can see the tab where buttons are located. Therefore, such a policy is useful if no Internet Control Panel policy hides the tab where the corresponding button is located.

The following eight policies control settings in the General Tab: *Disable changing home page settings, Disable changing Temporary Internet files settings, Disable changing history settings, Disable changing colour settings, Disable changing link colour settings, Disable changing font settings, Disable changing language settings,* and *Disable changing accessibility.*

No policies here control settings in the Security tab; zone policies are computer policies — see Section 9.3.

The following five policies control settings in the Content tab: *Disable changing rating settings, Disable changing certificate settings, Disable changingProfile Assistant settings, Disable Autocomplete for forms*, and *Do not allow Autocomplete to save passwords.*

The following five policies control settings in the Connections tab: *Use Automatic Detection for dial-up connections, Disable Internet Connection wizard, Disable changing connections settings, Disable changing proxy settings,* and *Disable changing Automatic Configuration settings.*

The following four policies control settings in the Programs tab: *Disable changing Messaging settings, Disable changing Calendar and Contact settings, Disable the Reset Web Settings feature,* and *Disable changing default Browser Check.*

P517531.PDF [Page: 73 of 85]

The following policy control settings in the Advanced tab: *Disable changing* and *Advanced page settings.*

Note: Among the seven other policies, only two policies are important with respect to security: Disable caching of Auto-Proxy scripts and Display error message on proxy script download failure.

9.2.3 Policies in Offline Pages node

A channel is a schedule and a URL to a Web page. Channels are used for updating automatically Web pages on computers. IE can create and delete channels. After its creation, a specific process on a computer to download the updated version of the Web page at the scheduled time uses the channel. Offlines Pages policies are policies that control channel behaviours. Figure 42 shows these policies.

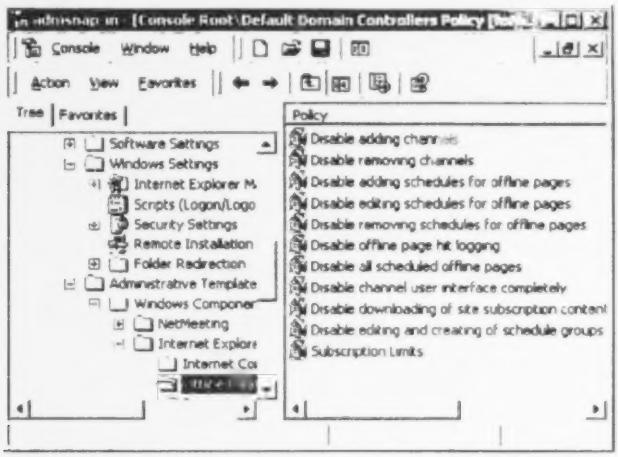

Figure 42: Offline Pages policies

9.2.4 Policies in Browser menus node

In the Browser menus node, almost all policies control some options that are accessible to users.

The *Disable Save this program to disk option policy* is worth some more comments. For security purpose, an administrator may enable this policy to disallow downloads of programs, which can be malicious.

P517531.PDF [Page: 74 of 85]

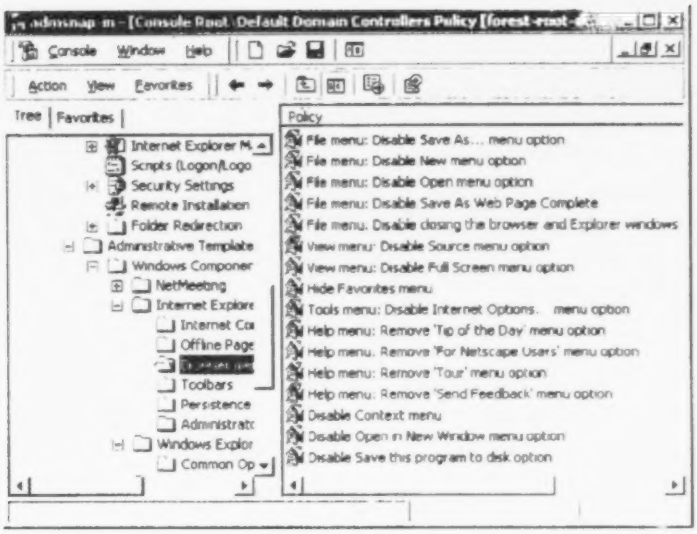
Console Root\Default Domain Controllers Policy [forest-root-
Console Window Help
Action View Favorites
Tree Favorites
Policy
Internet Explorer M
Scripts (Logon/Logo
Security Settings
Remote Installation
Folder Redirection
Administrative Template
Windows Componer
NetMeeting
Internet Explore
Internet Co
Offline Page
Toolbars
Persistence
Administratc
Windows Explor
Common Op
File menu: Disable Save As... menu option
File menu: Disable New menu option
File menu: Disable Open menu option
File menu: Disable Save As Web Page Complete
File menu: Disable closing the browser and Explorer windows
View menu: Disable Source menu option
View menu: Disable Full Screen menu option
Hide Favorites menu
Tools menu: Disable Internet Options... menu option
Help menu: Remove 'Tip of the Day' menu option
Help menu: Remove 'For Netscape Users' menu option
Help menu: Remove 'Tour' menu option
Help menu: Remove 'Send Feedback' menu option
Disable Context menu
Disable Open in New Window menu option
Disable Save this program to disk option

Figure 43: Policies in Browser menus node

9.2.5 Policies in Toolbars node

As shown in Figure 44, there are only three Toolbars policies. If the *Configure Toolbar Buttons* policy is enabled, we can select which toolbar buttons are to be displayed to users. Figure 45 shows which buttons can be selected. Other policies are used to disallow toolbar customisation from users.

Note: Toolbar policies are not important with respect to security.

P517531.PDF [Page: 75 of 85]

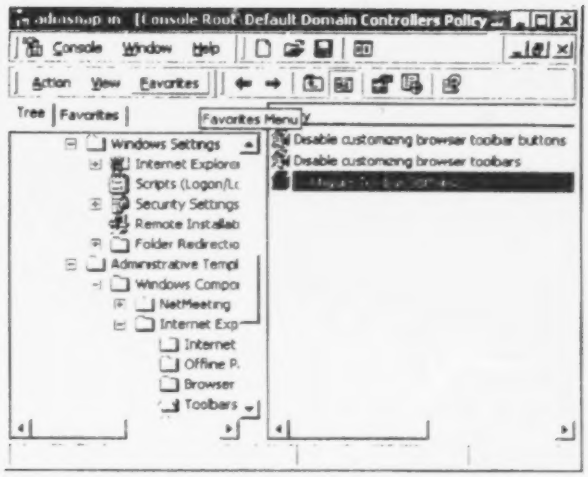

Figure 44: Toolbars policies

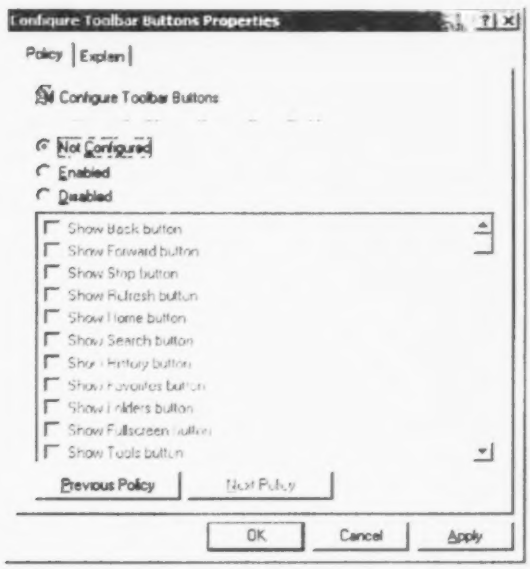

Figure 45: Toolbar Buttons selection

9.2.6 Policies in Persitance Behaviours node

These policies control the file size limits for the following five zones: Local Machine, Intranet, Trusted Sites, Internet, and Restricted Sites.

Note: These policies are not important with respect to security.

P517531.PDF [Page: 76 of 85]

9.2.7 Policies in Administrator Approved Controls node

For each ActiveX control shown in the right panel of Figure 46, a policy is associated. If such a policy is enabled, the ActiveX control becomes administrator approved and can be run in security zones specified by administrators.

To specify how administrator-approved controls are handled for each security zone, carry out the following steps:

- In a Group Policy, click User Configuration, click Internet Explorer Maintenance, and then click Security.
- Double-click Security Zones and Content Ratings, click Import the Current Security Zones Settings, and then click Modify Settings.
- Select the content zone in which you want to manage ActiveX controls, and click Custom Level.
- In the Run Active X Controls and Plugs-ins area, click Administrator Approved.

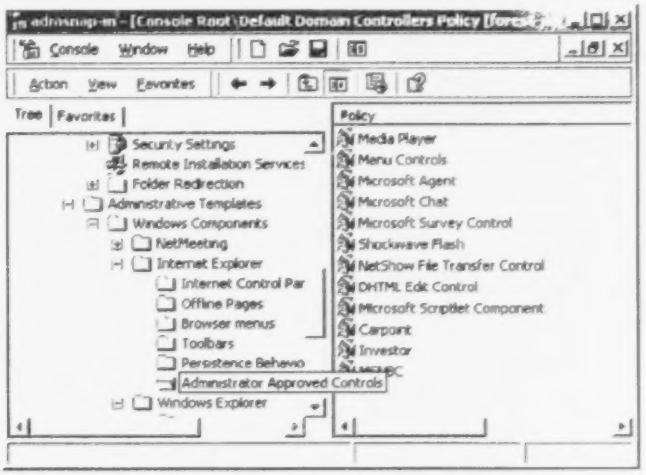

Figure 46: Administrator Approved Controls policies

Note: These policies are important with respect to security. Before administrators approve such controls, further study need to be conducted.

9.3 Computer settings in Windows Settings node

As shown in Figure 47, there are eight computer policies that apply to Internet Explorer.

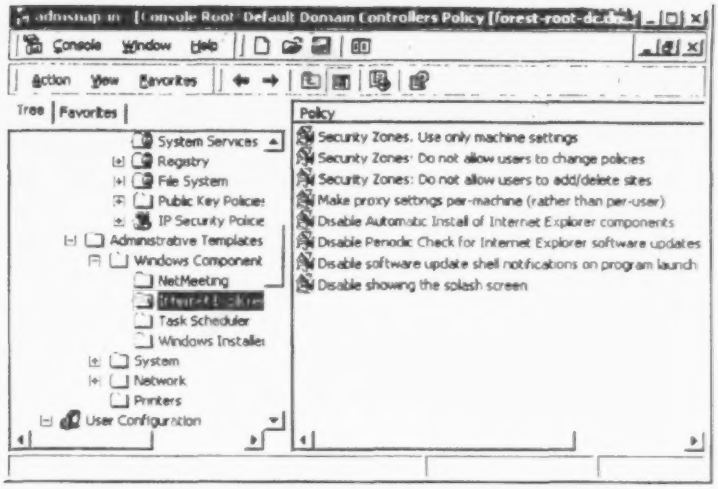

Figure 47: Policies in Computer Internet Explorer node

We analyse here only the first four policies, which are the ones important with respect to security. Three of these four policies are related to zones. Before analysing them, let us see when browsers use zones. When a browser connects to a site, it sets its security settings with respect to the site zone. A site belongs to one of the following five zones: computer, local Intranet, trusted sites, Internet, and restricted sites — see Figure 48 — and each zone has a set of security settings. Figure 48 shows the security tab in the Internet Settings dialog box, in which zone settings can be made.

Zone security settings information is stored in both of the following two registry keys:

\HKLM\software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones

\HKCU\software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones.

Each of these registry keys is similar and contains five zone subkeys where each subkey contains the security settings for a zone. When a browser accesses a site, it loads the zone security settings from the corresponding zone subkey in one of these two keys.

If the *Security Zones: Use only machine setting* policy is enabled, the browser loads the zones' security settings from the \HKLM registry key shown above. If this policy is disabled, the browser loads them from the \HKCU registry key.

The *Security Zones: Do not allow users to change policies* policy when enabled controls the Custom Level button shown in Figure 48. If this policy is enabled, users cannot customize security levels from the Security tab for any of the four zones shown in Figure 48. However, all users can modify directly their zone settings in the

P517531.PDF [Page: 78 of 85]

their \HKCU registry key and only privileged users can modify directly zones settings in the \HKLM registry key. Therefore, this policy is not really valuable if the *Security Zones: Use only machine setting* policy is not enabled because a user can modify the browser's zone security settings directly.

The *Security Zones: Do not allow users to add/delete sites* policy when enabled controls the Sites button in Figure 48. If this policy is enabled, users cannot add or delete sites from this interface.

If the *Make proxy setting per-machine* policy is enabled, the proxy settings are the same for all users on a computer. Proxy settings are contained in the connection registry key.

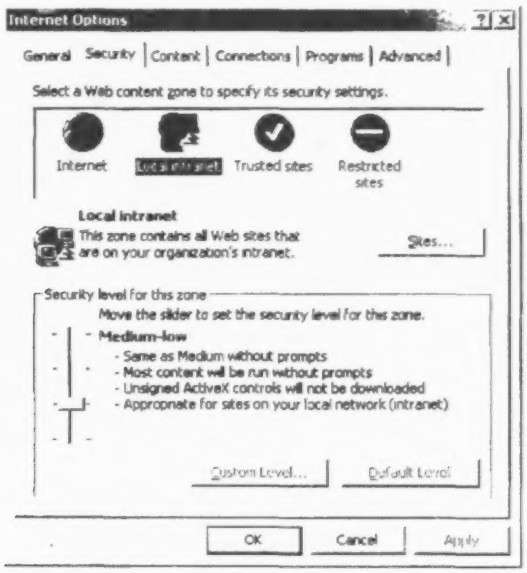

Figure 48: Internet Options' Security tab

10. Adm files

In this section, we provide information on adm files that can be useful for those that want to create new Administrative Templates policies or see a comparison between adm files for Windows 2000 and Windows NT.

10.1 Editing and using adm files

A Windows 2000 adm file is either an ASCII or a Unicode text file. Unicode support is new in Windows 2000. There are three adm files currently provided by Microsoft: System.adm, Inestres.adm, and Conf.adm. Together, they contain more than 450 setting appropriate to Windows 2000. Inestres.adm and Conf.adm contain settings respectively for Internet Explorer and Netmeeting, and System.adm contains various settings.

Adm files can be edited by using a text editor such as NOTEPAD.EXE in which a text file can be saved as either an Ansi or a Unicode text file. Adm files used by the Group Policy snap-in for Windows 2000 and by the POLEDIT.EXE utility for Windowns NT are very similar. Nevertheless, even though it is possible to load both a Windows 2000 ASCII adm file in the Windows NT policy editor and a Windows NT adm file in the Group Policy snap-in, the result will not be the one expected. Indeed, each policy section in adm files for Windows 2000 contains version information. When POLEDIT.EXE reads such sections, it reads only sections with version number lower or equal to 2; other sections are ignored. On the other hand, when the Group Policy snap-in reads a Windows NT adm file, no version appears in the adm file. Then, the snap-in assumes that that all policy sections have a version lower or equal to 2. For the current Group Policy snap-in, only policies defined in policy sections with version number equal to 3 are applied to the registry; other policies are not considered.

Note: It is easy to modify a Windows 2000 adm file to get a Windows NT adm file. It is sufficient to delete the version information with the associated endif.

10.2 Saving adm files

The Administrative Templates extension of Group Policy saves information in the Group Policy's adm files in two files named both Registry.pol. The first Registry.pol file is located in the Group Policy folder's Machine folder and contains the registry settings that are applied to computers. The second Registry.pol file is located in the Group Policy folder's User folder and contains the registry settings that are applied to users.

Registry.pol files are not text files. Moreover, policy files created by Windows NT 4.0 and Windows 2000 can be applied only to the operating system on which they were created.

P517531.PDF [Page: 80 of 85]

11. Conclusion

As said in the introduction, the next step after this technical memorandum is to build one or more domain demonstrators providing examples of secure Windows 2000 domains that could be used by the Canadian Forces and other Canadian government organisations. In order to achieve a first domain demonstrator some suggestions and points to consider are listed below.

1. Create a Windows 2000 domain demonstrator mimicking/replacing a set of one or more existing Windows NT 4.0 domains within DND. These Windows NT 4.0 domains should be domains in which security is important.

2. Determine applications and servers that are used within these Windows NT 4.0 domains.

3. For each application that is not an administrator applications, check if the application or a new version of the application can be run with simple user privileges and rights. If it is the case, it would be possible to assign to normal users only few privileges and rights. Otherwise, this is more complex. Assign the minimal set of privileges and rights to normal users. However, normal users should never belong to the administrator group because this group can modify the system security settings.

4. For applications and servers that need authentication, check if there are versions that use Kerberos. Kerberos is a better authentication mechanism than the one provided by LanManager. If it is not the case, authentication policies would have to be relaxed and the security would be lower.

5. Services and applications should be managed centrally. So, administrators would have to provide installation files and installation policies. Installation policies are defined in Windows Installer nodes.

6. System files should be read-only access to normal users.

7. If Internet Explorer is used, policies on Internet Explorer should be set up to protect the system and users.

P517531.PDF [Page: 81 of 85]

References

1. Savoie, J. (2001). Windows NT 4.0 and 2000 security (DREO TN-2001-086). Defence Research Establishment Ottawa.

2. Cox, P, and Sheldon, T.(2001). Windows 2000 security handbook. First ed. Berkeley, California: Osborne/MacGraw-Hill USA.

3. Ivens, K, and Gardiner, K. (2000). Windows 2000: The complete reference. First ed. Berkeley, California: Osborne/MacGraw-Hill USA.

4. Microsoft Inc. (2000). Microsoft Windows 2000 Server Resource Kit, Microsoft Press.

5. National Security Agency. (Online) Windows 2000 Security Recommendation Guides, http://nsa2.www.conxion.com/win2k/download.htlm (Oct. 16, 2001).

P517531.PDF [Page: 82 of 85]

List of acronyms

COM	Component Object Model
DC	Domain Controller
DLL	Dynamic Link Library
GPO	Group Policy Object
GUID	Globally Unique IDentifier
HKCU	HKEY_CURRENT_USER
HKLM	HKEY_LOCAL_MACHINE
IE	Internet Explorer
ISV	Independent Software Vendor
MMC	Microsoft Management Console

UNCLASSIFIED
SECURITY CLASSIFICATION OF FORM
(highest classification of Title, Abstract, Keywords)

DOCUMENT CONTROL DATA

(Security classification of title, body of abstract and indexing annotation must be entered when the overall document is classified)

1. ORIGINATOR (the name and address of the organization preparing the document Organizations for whom the document was prepared, e g Establishment sponsoring a contractor's report, or tasking agency, are entered in section 8)

Defence Research Establishment Ottawa
Ottawa, Ontario
Canada K1A 0Z4

2. SECURITY CLASSIFICATION (overall security classification of the document, including special warning terms if applicable)

UNCLASSIFIED

3. TITLE (the complete document title as indicated on the title page. Its classification should be indicated by the appropriate abbreviation (S,C or U) in parentheses after the title.)

A Security Analysis of Windows 2000 Group Policies (U)

4. AUTHORS (Last name, first name, middle initial)

Savoie, Jean

5. DATE OF PUBLICATION (month and year of publication of document)

November 2001

6a. NO OF PAGES (total containing information. Include Annexes, Appendices, etc)

75

6b. NO. OF REFS (total cited in document)

5

7. DESCRIPTIVE NOTES (the category of the document, e g technical report, technical note or memorandum. If appropriate, enter the type of report, e.g. interim, progress, summary, annual or final. Give the inclusive dates when a specific reporting period is covered)

DREO Technical Memorandum

8. SPONSORING ACTIVITY (the name of the department project office or laboratory sponsoring the research and development Include the address.)

Information Operations Section
Defence Research Establishment Ottawa
Ottawa ON Canada K1A 0Z4

9a. PROJECT OR GRANT NO (if appropriate, the applicable research and development project or grant number under which the document was written Please specify whether project or grant)

15BF27

9b. CONTRACT NO. (if appropriate, the applicable number under which the document was written)

10a. ORIGINATOR'S DOCUMENT NUMBER (the official document number by which the document is identified by the onginating activity This number must be unique to this document)

DREO TM 2001-084

10b. OTHER DOCUMENT NOS. (Any other numbers which may be assigned this document either by the originator or by the sponsor)

11. DOCUMENT AVAILABILITY (any limitations on further dissemination of the document, other than those imposed by security classification)

(X) Unlimited distribution
( ) Distribution limited to defence departments and defence contractors, further distribution only as approved
( ) Distribution limited to defence departments and Canadian defence contractors, further distribution only as approved
( ) Distribution limited to government departments and agencies, further distribution only as approved
( ) Distribution limited to defence departments; further distribution only as approved
( ) Other (please specify):

12. DOCUMENT ANNOUNCEMENT (any limitation to the bibliographic announcement of this document This will normally correspond to the Document Availability (11). However, where further distribution (beyond the audience specified in 11) is possible, a wider announcement audience may be selected)

Full Unlimited Announcement

P517531.PDF [Page: 84 of 85]

13. ABSTRACT (a bnef and factual summary of the document It may also appear elsewhere in the body of the document itself. It is highly desirable that the abstract of classified documents be unclassified Each paragraph of the abstract shall begin with an indication of the security classification of the information in the paragraph (unless the document itself is unclassified) represented as (S), (C), or (U) It is not necessary to include here abstracts in both official languages unless the text is bilingual)

In this technical memorandum, we analyse the security-relevant Windows 2000 policies that can be set up on Windows 2000 domains and show how those policies are applied and implemented. These policies are a large set of authentication policies, password policies, application policies, installation policies, and others.

This analysis is a first step needed before setting up the Windows 2000 policies for one or more secure domain demonstrators for the Canadian Forces and other organisations where normal users would be low power users to mitigate risk on domain assets.

14. KEYWORDS, DESCRIPTORS or IDENTIFIERS (technically meaningful terms or short phrases that characterize a document and could be helpful in cataloguing the document They should be selected so that no security classification is required. Identifiers such as equipment model designation, trade name, military project code name, geographic location may also be included. If possible keywords should be selecte from a published thesaurus. e.g Thesaurus of Engineering and Scientific Terms (TEST) and that thesaurus-identified If it is not possible to select indexing terms which are Unclassified, the classification of each should be indicated as with the title)

Windows 2000, domain, domain policy, group policy, network policy

P517531.PDF [Page: 85 of 85]

Defence R&D Canada
is the national authority for providing
Science and Technology (S&T) leadership
in the advancement and maintenance
of Canada's defence capabilities.

R et D pour la défense Canada
est responsable, au niveau national, pour
les sciences et la technologie (S et T)
au service de l'avancement et du maintien des
capacités de défense du Canada.

P 517531
CA020804

DEFENCE R&D DÉFENSE

www.drdc-rddc.dnd.ca